Sujet élaboré par une cellule pédagogique nationale

CONCOURS EXTERNE D'ATTACHÉ TERRITORIAL

SESSION 2022

ÉPREUVE DE NOTE

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'une note ayant pour objet de vérifier l'aptitude à l'analyse d'un dossier portant sur la conception et la mise en place d'une application automatisée dans une collectivité territoriale.

Durée : 4 heures
Coefficient : 4

SPÉCIALITÉ : ANALYSTE

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 39 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

Attaché territorial, vous êtes nommé chargé de mission transformation numérique, rattaché à la Direction des Systèmes d'Information (DSI) de la ville d'Admiville (80 000 habitants).

Suite à des incidents répétés (pannes de serveurs, lenteurs du réseau…), notamment liés à l'obsolescence technique de la salle informatique, le Directeur des Systèmes d'Information, vous confie comme première mission une étude sur l'opportunité du déploiement de l'informatique en nuage (cloud computing).

A cet effet, il vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, une note sur le recours à l'informatique en nuage dans les collectivités territoriales.

Liste des documents :

Document 1 : « Le cloud pollue davantage qu'un simple nuage » – *siecledigital.fr* – 1er décembre 2021 – 4 pages

Document 2 : « Data Centers et économie d'énergie : sont-ils vraiment des « ogres numériques » en termes d'écologie ? » – *data4group.com* – 13 décembre 2018 – 2 pages

Document 3 : « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing » (extrait) – *cnil.fr* – janvier 2019 – 10 pages

Document 4 : « Sécurité cloud : le guide des outils essentiels et des bonnes pratiques » – *zdnet.fr* – 22 juillet 2021 – 4 pages

Document 5 : « Cloud souverain, trois niveaux sinon rien ? » – *aucoeurdesmétiers.fr* – octobre 2019 – 1 page

Document 6 : « Optimiser sa stratégie de sourcing cloud » – *decisions-achats.fr* – avril 2018 – 2 pages

Document 7 : « Pourquoi les collectivités doivent s'intéresser au cloud souverain » – *zdnet.fr* – 18 juin 2021 – 2 pages

Document 8 : « Les collectivités pourront récupérer la TVA sur les services IaaS » – *solutions-numériques.com* – 28 juillet 2020 – *2* pages

Document 9 : « Le cloud computing, dissipons les nuages » – *lagazettedescommunes.com* – avril 2019 – 1 page

Document 10 : « Une limitation de l'éligibilité au FCTVA des dépenses de cloud engagées par les *collectivités ? » lagazettedescommunes.com* – 26 octobre 2021 – 1 page

Document 11 : « Le paradoxe du cloud : réduire les coûts, mais dépenser plus » – *itforbusiness.fr* – 8 mars 2018 – 1 page

Document 12 : « La cybersécurité des entreprises – Prévenir et guérir : quels remèdes contre les cyber virus ? » (extrait) – *senat.fr* – 21 juin 2021 – 2 pages

Document 13 : « Le gouvernement adopte le cloud pour un stockage ultra-sécurisé des données » – *weka.fr* – 9 juin 2021 – 1 page

Document 14 : « Loi n°2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France (REEN) » – *kiosque.bercy.gouv.fr* – 15 novembre 2021 – 2 pages

Document 15 : « Incendie et perte de données, les clients d'OVH confrontés aux limites contractuelles » – *usinenouvelle.com* – 23 mars 2021 – 2 pages

DOCUMENT 1

Le cloud pollue davantage qu'un simple nuage

Les services cloud s'appuient sur de nombreux serveurs répartis à travers le monde. Contrairement aux déchets pour lesquels les impacts environnementaux sont directement visibles, ceux du matériel informatique le sont moins. Néanmoins, ils ne sont pas pour autant inexistants.

Par Julia Guinamard - @GuinamardJM
Publié le 6 avril 2021 à 08h12 - Mis à jour le 1 décembre 2021 à 17h35
siecledigital.fr

« Passer de l'informatique sur site au cloud, c'est comme passer de la voiture individuelle aux transports en commun », résument Stanislas de Rémur, Édouard de Rémur et Cédric Mermilliod dans leur livre Pour un cloud européen. Une exception est néanmoins à préciser, passer de l'informatique traditionnelle au cloud, contrairement à passer de la voiture aux transports en commun, n'est pas nécessairement écologique. Souvent, les internautes ont déjà en leur possession du matériel leur permettant de stocker leurs données : clé USB, disque dur, mémoire vive, etc. En passant par des services de cloud, c'est comme si ces équipements étaient dupliqués, ce qui demande bien évidemment de l'énergie. La question du besoin doit être réfléchie. « Est-ce que les photos de vacances ont vraiment besoin d'être stockées sur le cloud ? », interroge Maxime Guedj, ingénieur, entrepreneur et co-auteur de Déclic, Comment profiter du numérique sans tomber dans le piège des géants du web.

Selon un rapport (PDF) de la Commission européenne, en 2010, en Europe, les services cloud représentaient 10% de la consommation des centres de données. Près de 10 ans plus tard, en 2018, ils représentaient 35% de la consommation des data centers. Entre 2010 et 2018, la consommation énergétique des data centers des 28 pays européens est passée de 53,9 TWh/an à 76,8 TWh/an, soit une hausse de 42%.

Le mot cloud renvoie une image dématérialisée de l'informatique. Une projection trompeuse, comme le rappelle la construction de nombreux data centers à travers le monde. Derrière le cloud se trouvent des millions d'ordinateurs, de smartphones, de data centers, et des kilomètres de réseaux. Un tableau bien loin de l'immatérialité induite par le mot. Selon Françoise Berthoud, informaticienne au Gricad, relayée par CNRS Le Journal, le secteur des nouvelles technologies représente entre 6% et 10% de la consommation mondiale d'électricité, soit environ 4% des gaz à effet de serre. Tous les ans ce chiffre augmente d'entre 5% et 7%. Parmi les 6% à 10% de la consommation mondiale d'électricité, 30% concernent les ordinateurs, smartphones et objets connectés, 30% reviennent aux data centers, et le reste, 40% sont attribués aux infrastructures réseaux, soit les câbles qui acheminent les données.

Pour l'internaute, cette externalisation de l'informatique complexifie l'appréhension de l'empreinte carbone du numérique. L'utilisateur ne voit pas le remplacement, en moyenne, des serveurs tous les 5 ans, ni les problématiques de recyclage. Seulement 18% des métaux d'un ordinateur portable sont récupérés. Beaucoup de matériaux finissent dans des décharges sauvages, notamment en Chine, en Inde, et au Ghana, où ils sont brûlés pour récupérer certains matériaux, ce qui engendre, notamment, une pollution des nappes phréatiques. Le matériel informatique nécessite de nombreux composants : or, cuivre, nickel, zinc, étain, arsenic, gallium, germanium, thallium, tantale, indium, etc. Comme dans la majorité des industries extractives, les conséquences environnementales sont nombreuses, notamment à cause de l'utilisation de produits nocifs pour les écosystèmes, comme l'acide sulfurique, le mercure, ou encore le cyanure.

Les services cloud pourraient être comparés à l'achat d'une fourchette en plastique pour un pique-nique. D'un point de vue global, ramener sa propre fourchette réutilisable demande moins d'énergie. Mais du point de vue du consommateur, prendre une fourchette jetable est simple, cela évite une vaisselle. Dans le cas du plastique, la gestion des déchets a été externalisée. Envoyée à l'autre bout du monde, sa pollution a été masquée. Avec le numérique, la dynamique est similaire. La délocalisation du stockage et de la puissance de calcul dans des centres de données rend toute une partie de l'informatique invisible aux yeux de l'utilisateur.

« Il existe en effet un grand malentendu entre deux définitions de la neutralité carbone qui coexistent »

Aujourd'hui, les politiques environnementales des entreprises constituent des arguments de vente. Google revendique tendre vers le zéro déchet et être neutre carbone depuis 2007. Pour le premier point, dans une industrie qui utilise beaucoup de composants difficilement recyclables, tendre vers du zéro

déchet est ambitieux, voire paradoxal. En 2016, Google revendiquait six data centers comme zéro déchet sans apporter trop de précisions. Pour cet objectif de zéro déchet, l'entreprise a mis en avant que 52 % des composants utilisés pour des améliorations de performance des serveurs provenaient déjà d'anciens serveurs. Néanmoins, 48 % demeurent loin de zéro.

L'engagement sur le long terme et le plus concret de Google reste la neutralité carbone. Avant d'applaudir l'engagement écologique, il est important de s'attarder sur la définition de neutralité carbone des entreprises. La neutralité carbone repose sur le postulat qu'une tonne de gaz à effet de serre (GES) a le même impact sur le climat peu importe l'endroit ou les conditions de son émission. De la même manière, la compensation d'émissions de GES a le même impact peu importe la situation. Sur cette base, les entreprises polluantes peuvent acheter du crédit carbone sur des marchés afin de compenser leurs émissions, et ainsi déclarer une neutralité. Cette neutralité relève donc avant tout d'une compensation de la pollution et non de sa réduction. C'est une forme d'achat de droit de polluer. Siècle Digital a interrogé Google sur cette nuance qui répond à l'écrit : « Renvoyer vers la définition de la neutralité carbone généralement acceptée (politiques, associations, milieux économiques etc) ».

« Il existe en effet un grand malentendu entre deux définitions de la neutralité carbone qui coexistent. D'un côté, il y la notion de neutralité carbone des entreprises, qui a émergé il y a une quinzaine d'années dans la foulée du protocole de Kyoto, et qui repose essentiellement sur la compensation carbone. De l'autre, il y a la neutralité carbone au sens de la science, qui est l'équilibre entre les émissions et les absorptions de CO2 à l'échelle mondiale, et qui est d'une ambition radicale. Les deux ne coïncident pas et c'est très dommageable : une entreprise qui se dit 'neutre' aujourd'hui n'est pas forcément alignée avec l'ambition de l'Accord de Paris », explique à Novethic César Dugast, membre de Carbone 4.

GAFAM : conscience écologique ou greenwashing ?

Dans la même lignée, Microsoft a annoncé aller plus loin que Google en devenant négatif en carbone d'ici 2030, c'est-à-dire compenser plus de CO2 que l'entreprise en produit. Par ailleurs, l'entreprise travaille sur des piles à hydrogène pour alimenter les data centers. En juillet 2020, Microsoft a réussi à alimenter plusieurs serveurs d'un data center grâce à cette technologie. D'un point de vue écologique, cette réussite demande des vérifications, notamment sur le CO2 émis pour construire les piles à hydrogène. Néanmoins, il ne faut pas enlever à Microsoft que l'hydrogène se présente de plus en plus comme une alternative énergétique concluante et qu'investir dans ce domaine aide la recherche.

En 2018, Google et Apple ont annoncé être alimentés à 100% par des énergies renouvelables. Avant de crier victoire, il faut noter que les énergies à sources renouvelables ne sont pas forcément plus écologiques : elles demandent de l'espace, nécessitent des matériaux rares, etc. De plus, le caractère intermittent du solaire et de l'éolien demande le recours à des énergies pilotables pour assurer de l'électricité en continu. Si l'hydraulique est à la fois renouvelable et pilotable, les autres solutions pilotables se concentrent sur le nucléaire, le gaz naturel - aussi appelé gaz fossile - ou encore sur le charbon. Par ailleurs, pour l'hydraulique, il est important de rappeler que pour la construction d'une centrale, des espaces sont inondés, ce qui dégage du CO2 à cause de la méthanisation intervenant à la suite de la décomposition des végétaux.

Immerger des serveurs pour les refroidir

« Un processeur, c'est comme une résistance. Presque toute l'électricité qu'il consomme est dissipée en chaleur. C'est pourquoi, en plus de consommer de l'énergie pour faire tourner ses serveurs, un data center doit être climatisé afin de préserver l'intégrité des circuits électroniques », explique à *CNRS Le Journal* Anne-Cécile Orgerie, chercheuse à l'Institut de recherche en informatique et systèmes aléatoires (Irisa).

Cet enjeu de refroidissement des data centers est bien connu de la part des acteurs de la tech qui cherchent des solutions, notamment en immergeant des serveurs dans de l'eau ou des liquides de refroidissement. Plonger des composants électriques dans un liquide, n'apparaît pas comme la meilleure idée, Claude François l'a démontré. L'idée, en vulgarisant, est que pour rafraîchir une bière ce n'est pas l'ensemble de l'environnement dans lequel se trouve la boisson qui est refroidie. L'option la plus évidente est de placer les bouteilles dans un réfrigérateur. Dans un scénario en pleine nature, les bouteilles peuvent être déposées dans l'eau froide de la mer ou d'une rivière.

En novembre 2020, Microsoft a annoncé le succès du projet Natick, un data center aquatique immergé au large des côtes écossaises pendant 2 ans. Néanmoins, l'écologiste Gordon Watson nuance cette avancée en mettant en avant le manque d'étude sur l'impact sur les écosystèmes. En France, l'entreprise TotaLinuX développe le programme ITrium. Évoqué comme une usine numérique, ITrium comprend un bâtiment regroupant à la fois des bureaux, des salles de conférences et un data center immergé dans un liquide de refroidissement. La chaleur émise par le data center est réduite, la température des équipements est stabilisée et le matériel est protégé de l'humidité et de la poussière.

Refroidir les data centers avec l'eau des nappes phréatiques

Au lieu d'avoir des températures pouvant monter jusqu'à 60°C ou 70°C, le data center d'ITrium ne dépasse pas 25°C. De fait, la consommation électrique utilisée pour refroidir les serveurs diminue. La chaleur émise par l'effet de joule [ndr : chaleur produite par l'électricité quand elle traverse un corps], dégagée par les serveurs, est utilisée pour chauffer les bureaux et salles de conférence du bâtiment. Plongé dans le liquide, le bruit émis par les serveurs baisse considérablement. À ces bénéfices s'ajoute le fait que la durée de vie des composants électroniques est allongée à 9 ans, contre 3 à 5 ans pour les data centers à refroidissement par air.

Le liquide de refroidissement utilisé par ITrium est un isolant qui ne s'évapore pas et bénéficie d'une durée de vie de 25 ans. Au terme du cycle, les groupes pétroliers, auxquels se fournit TotaLinuX, récupèrent le liquide et se chargent du recyclage. La formule chimique du liquide est confidentielle et détenue par les raffineurs produisant le liquide : Total, Shell, et Texaco. En tant que client, TotaLinuX a accès aux éléments de la formule sans pour autant connaître leur proportion. Le liquide est certifié biodégradable au bout de 28 jours, ce qui est particulièrement important en cas d'une fuite accidentelle.

Certains centres de données profitent de leur environnement naturel. C'est le cas du Green Center Eolas qui utilise l'eau des nappes phréatiques pour refroidir son data center. *« On puise de l'eau qui est souterraine, à 14°C, elle entre dans notre process de refroidissement pour produire de l'eau qui va jusqu'aux équipements informatiques pour les refroidir »*, explique à *France 3* Bruno Touzain, responsable d'exploitation du Green Center Eolas. En puisant l'eau de la nappe phréatique, trois fois moins d'énergies est utilisée par rapport aux centres à refroidissement par air. En outre, l'entreprise se fournit en énergie auprès d'un fournisseur qui donne accès à du 100% renouvelable. Dans d'autres cas, les centres de données tirent avantage d'anciennes installations, comme le data center parisien de Scaleway qui est situé dans un ancien abri antiatomique et qui chauffe l'immeuble au-dessus duquel il est situé.

« Les éco-TIC sont loin d'être des baguettes magiques à verdir la planète »

Sans grande surprise, l'énergie utilisée par les data centers varie selon leur taille. Un centre de moindre envergure peut fonctionner avec quelques kilowatts d'énergie. Ceux de plus grande taille peuvent demander au moins des dizaines de mégawatts. Pour estimer l'efficacité d'un centre de données, il existe un indicateur d'efficacité énergétique : le Power usage effectiveness (PUE), soit en français l'efficacité de l'utilisation de l'énergie. Le PUE établit un ratio entre l'énergie totale consommée par le centre informatique et l'énergie consommée par les équipements informatiques. En France, en moyenne, le PUE des data centers s'élève à 2,5. Cela signifie que pour 1 watt consommé par le matériel informatique, il faut 2,5 watts à l'entrée du data center. Le PUE mesure donc le rendement d'un centre de traitement et ne fait pas référence à une économie d'énergie. Cet indicateur a été élaboré par le consortium The Green Grid, qui compte parmi ses membres des géants de l'informatique comme IBM, Intel, Dell, Hewlett Packard (HP), ou encore Nvidia.

Pour estimer l'empreinte carbone des services cloud, se concentrer uniquement sur l'énergie utilisée par les data centers n'est pas suffisant. L'impact de la fabrication du matériel informatique représenterait entre 50 et 75% de l'empreinte carbone du numérique. Estimer une empreinte carbone est très complexe, et demande d'accepter certaines hypothèses et d'en écarter d'autres. Dans le cas d'un ordinateur, prendre en compte l'extraction minière est essentiel. Mais est-ce que l'essence utilisée pour acheminer les terres rares à l'usine de transformation est comptée ? De manière encore plus poussée, est-ce que l'essence du salarié qui se déplace pour venir sur son lieu de travail et faire la publicité de l'ordinateur est prise en compte ?

Le groupe de travail GDS EcoInfo - soutenu par deux instituts du CNRS, celui des sciences de l'information et de leurs interactions et celui de l'écologie et l'environnement, se montre critique face à un numérique dit écologique et met la lumière sur les effets rebond : *« Les éco-TIC sont loin d'être des baguettes magiques*

à verdir la planète. En effet, elles comportent de sérieuses limites, dont la principale semble être l'existence d' "effets rebond", qui annulent tout ou partie de leurs bénéfices écologiques. Dans le cas des technologies numériques comme les serveurs, les gains en termes d'amélioration de l'efficacité énergétique pourraient donc être absorbés par une augmentation de la demande de stockage numérique d'informations, ce qui annulerait les bénéfices environnementaux de ces gains ».

« Lorsque la mémoire était comptée, les développeurs informatiques avaient l'habitude d'écrire du code synthétique et efficace »

Ce phénomène d'effets rebond a déjà été observé dans le développement de l'industrie automobile. Les progrès sur la puissance des véhicules a servi à leur ajouter des options, et donc de nouveaux usages, avec des composants alourdissant d'autant plus les voitures, qui nécessitent donc encore plus de puissance. *« Réduire la consommation des voitures n'a pas permis d'utiliser moins d'essence, elle a juste permis aux automobilistes de faire plus de kilomètres [...] On constate la même chose depuis des années dans le secteur des nouvelles technologies : plus on optimise les systèmes – la mémoire, le stockage, etc. –, plus on favorise de nouveaux usages »*, explique à *CNRS Le Journal* Anne-Cécile Orgerie.

La croissance du modèle SaaS est un exemple de ces nouveaux usages. Aujourd'hui, comme en témoigne le commencement de la course à la 6G alors même que la 5G n'est pas encore pleinement déployée, la puissance de calcul est le but ultime comme l'a été la vitesse dans l'automobile. Même si les data centers deviennent plus écologiques, l'augmentation continue de leur utilisation et les nouvelles possibilités offertes ne vont pas réellement réduire leur impact sur l'environnement.

« Lorsque la mémoire était comptée, les développeurs informatiques avaient l'habitude d'écrire du code synthétique et efficace. Aujourd'hui, ces préoccupations ont disparu et l'on assiste à une véritable inflation des lignes de code, ce qui signifie des calculs plus longs et plus gourmands en électricité », détaille Anne-Cécile Orgerie. Quand internet était lent, il y avait beaucoup plus d'efforts pour compresser les données. En effet, si le contenu est plus léger, l'envoi est aussi plus rapide. Une fois compressée, la donnée nécessite beaucoup moins de place, et, de fait, moins de serveurs. Aujourd'hui, alors que la tendance est à un internet toujours plus rapide, les données sont de moins en moins compressées. Néanmoins, il faut prendre en compte que compresser des données demande un travail de calcul, qui a lui aussi une empreinte écologique.

« Or, même inactifs, ces équipements sont très énergivores »

Cette question de compresser les données se retrouve dans le secteur de l'Internet des Objets (IoT). Les formats JPEG compressent les images, mais demandent donc des ressources pour le traitement. Dans le cas d'objets de petite taille, cela incarne une problématique à résoudre. Sur ce point, le CS (Compressive Sensing) serait une piste intéressante à creuser pour limiter la puissance de calcul requise. Sur les ordinateurs les « bloatware » ou « obésiciels », qui sont de généralement des programmes installés par défaut, occupent souvent une place importante et demande beaucoup de ressources pour fonctionner.
Cela pourrait être réduit, tout comme l'ensemble des programmes informatiques. C'est d'ailleurs ce que propose l'entreprise nantaise Greenspector qui améliore la performance énergétique des applications web et mobiles. Autre initiative française, le Green Code Lab qui promeut l'éco-conception des logiciels.

La disponibilité constante des services est aussi à réfléchir. En effet, les infrastructures sont organisées pour faire face à des pics d'utilisation qui arrivent seulement à quelques heures de la journée. *« Or, même inactifs, ces équipements sont très énergivores »*, explique Anne-Cécile Orgerie dans *CNRS Le Journal*, qui déplore que *« malgré de nombreuses recherches qui affirment que cela n'affecterait pas la performance du service, les data centers continuent d'être à 100 % de leur capacité jour et nuit »*. Cette situation s'explique par la crainte des fournisseurs de services numériques de faire subir à leurs utilisateurs quelques secondes de latence ou un débit entrecoupé.

Utiliser un service cloud laisse de nombreuses responsabilités entre les mains des prestataires, dont celles d'ordre écologique. Il faut donc se demander si l'intérêt de l'entreprise est d'avoir un faible impact sur l'environnement ou d'offrir des services toujours plus performants. Le projet Blue Frontiers, porté par le groupe libertarien Seasteading Institute, qui consiste à créer des îles artificielles complètement intégrées à la végétation dans les eaux territoriales françaises, ou la volonté d'Elon Musk de coloniser Mars, laissent présager que les milliardaires propriétaires des grandes entreprises de la tech cherchent d'autres solutions au dérèglement climatique que la réduction de l'impact des activités humaines.

DOCUMENT 2

Data Centers et économie d'énergie :

sont-ils vraiment des "ogres numériques" en terme d'écologie ?

data4group.com – 13 décembre 2018

Ces dernières années, les centres de données ont considérablement gagné en performance. Si leur développement n'est certes pas sans conséquence en termes de consommation d'énergie, sont-ils pour autant des gouffres énergétiques ?

En 2015, le secteur du numérique consommait aux environs de 10% de la production énergétique mondiale, dont 18% consommés par l'ensemble des data centers, et les serveurs informatiques qu'ils abritent. Ces chiffres proviennent d'une synthèse publiée en 2017 par l'Association « négaWatt » dont l'objectif est l'abandon des énergies fossiles et nucléaires à l'horizon 2050.

Les centres de données, leurs infrastructures et leur consommation d'énergie

Les data centers sont des centres de stockage de données qui sont, en réalité, des endroits physiques où sont rassemblées plusieurs milliers d'unités centrales appelées serveurs. Ces derniers sont des machines reliées entre elles, c'est-à-dire, mises en réseau. L'objectif est de pouvoir héberger d'importants volumes de données numériques. La connexion Internet y est indispensable afin que les utilisateurs, souvent externes, puissent accéder aux données stockées dans ces serveurs. Au début de l'ère numérique, les entreprises disposaient en interne de leur propre serveur en réseau local. Le principe est le même que lorsque nous sauvegardons nos données dans le disque dur de notre propre ordinateur. Mais une telle structure qui emmagasine toujours plus de données demande un budget conséquent. D'autant plus que les risques de pannes mettent souvent en danger les entreprises. Désormais, les méthodes de sauvegarde ou d'hébergement de données ont évolué. Avec Internet, l'informatique dématérialisée devient une tendance : le « Cloud Computing ».

Le Cloud, ce système qui a tout changé

Le Cloud, qui signifie « nuage » en anglais, pourrait être défini comme un système virtuel de stockage ou d'hébergement. En réalité, il consiste à faire circuler vos données numériques, de votre disque dur, votre tablette ou votre smartphone vers un stockage déporté, regroupé dans un centre de données. Vos données, et même vos logiciels, sont alors disponibles à tout moment, où que vous vous trouviez à condition disposer d'une connexion Internet. La gestion des données devient ainsi plus facile pour les utilisateurs et les entreprises. L'externalisation de l'hébergement informatique est devenue naturellement une tendance lourde avec le volume grandissant de données qui circulent, notamment dans l'e-commerce où les sites web professionnels sont toujours disponibles sans interruption.

Selon une étude diffusée par Cisco, la capacité de stockage actuelle des centres de données ne suffira plus d'ici à 2021 : elle devrait être multipliée par 4. C'est dans ce contexte que les data centers deviennent de plus en plus stratégiques avec toutefois cette question grandissante sur leur réputation énergivore. Car il est vrai qu'il faut une quantité d'énergie importante pour faire tourner les machines en permanence et surtout, pour les refroidir efficacement.

Si la consommation d'énergie est inévitable, pourquoi ne pas récupérer la chaleur dissipée des Data centers ?

En 2015, l'Union française de l'électricité – UFE – indiquait que la consommation des data centers français avoisinait 3 TWh. C'est presque l'équivalent de la consommation électrique de la ville de Lyon. La moitié de cette consommation d'électricité est destinée au refroidissement et à la climatisation des data centers afin d'assurer la sécurité des données hébergées. Cette préoccupation est au cœur des professionnels du data center qui s'efforcent de diminuer le coût de la facture du refroidissement en optant, par exemple, pour le « free cooling » ou le refroidissement via l'air frais de l'extérieur. C'est le cas, par exemple, des serveurs délocalisés de Facebook qu'ils ont installés en Suède, les pays nordiques disposant d'un climat froid.

Exploiter la dissipation de chaleur pour le chauffage urbain

Bien sûr, l'effet Joule, c'est-à-dire, la manifestation thermique se produisant lors du passage du courant électrique dans n'importe quel conducteur, peut être exploité pour contrer les grosses dépenses engagées dans les systèmes de refroidissement. Cette chaleur produite peut être valorisée, par exemple, en l'utilisant comme chauffage urbain. Plusieurs endroits en France bénéficient déjà de cet usage spécifique. Entre autres, le quartier d'affaires de Val d'Europe, une résidence étudiante à Grenoble, mais aussi le chauffage d'une piscine publique à Paris. Bien que la technique soit encore assez limitée, elle constitue une avancée notable pour compenser les dépenses énergétiques induites par le fonctionnement des centres de données.

Les gains de performance et la valorisation de la chaleur dissipée sont autant de points positifs pour les centres de données. D'autant plus que, selon toujours le rapport de l'Association « négaWatt », d'autres infrastructures sont beaucoup plus énergivores que les data centers. À titre d'exemple, l'ensemble des terminaux utilisés, à savoir les ordinateurs, les tablettes et les smartphones, consommeraient à eux tous le double de l'énergie utilisée dans les centres de données.

Enfin, pour réduire davantage la consommation en énergie dans le secteur numérique, il est important de rappeler que chacun doit apporter sa contribution en adoptant des gestes simples au quotidien comme, par exemple, supprimer les anciens mails et notamment ceux comportant de grosses pièces jointes, ou en limitant la consommation de vidéos en streaming. En 2017, Le Parisien publiait les propos de l'analyste de Greenpeace, Gary Cook, indiquant que le visionnage seul du clip vidéo du chanteur coréen PSY, « Gangnam Style », a consommé l'équivalent de la production annuelle d'une modeste centrale électrique. Effectivement, cette vidéo a été visionnée plus de 2,5 milliards de fois dans le monde.

Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing (extrait) – *cnil.fr* – janvier 2019

(...)

D'un point de vue juridique, la CNIL constate que le Cloud computing soulève un certain nombre de difficultés au regard du respect de la législation relative à la protection des données personnelles, en particulier dans le cas du Cloud public. Ces difficultés sont amplifiées dans le cas des offres standardisées avec des contrats d'adhésion ne laissant pas aux clients la possibilité de les négocier. De manière générale, il est constaté que les clients souffrent d'une insuffisance de transparence de la part des prestataires de Cloud quant aux conditions de réalisation des prestations, notamment sur la sécurité et sur la question de savoir si leurs données sont transférées à l'étranger, et plus précisément à destination de quels pays.

Par conséquent, il est indispensable qu'une entreprise française qui envisage de recourir à un service de Cloud computing réalise une analyse de risques et soit très rigoureuse dans le choix de son prestataire. En particulier, l'entreprise devra prendre en considération les garanties offertes par un prestataire en matière de protection des données personnelles et s'assurer que ce dernier lui fournira toutes les garanties nécessaires au respect de ses obligations au regard de la loi Informatique et Libertés, notamment en termes d'information des personnes concernées, d'encadrement des transferts et de sécurité des données. Il est à noter qu'en cas d'impossibilité de négocier un contrat, une comparaison des conditions contractuelles proposées par les différents prestataires est indispensable. Ceci permet d'effectuer un choix prenant en compte les considérations tant économiques que juridiques et techniques.

Concernant la sécurité, la CNIL constate que les offres de Cloud reconnues peuvent présenter des niveaux de sécurité supérieurs à ceux que peuvent garantir les PME. Cependant, le Cloud génère de nouveaux risques, tant du côté du prestataire que du côté du client, notamment au niveau de la pérennité des données. Il est donc nécessaire de s'assurer que ces nouveaux risques sont maitrisés avant de choisir une solution de Cloud.

La CNIL a établi les recommandations suivantes afin d'aider les entreprises françaises, notamment les PME, à effectuer une prise de décision éclairée lorsqu'elles envisagent d'avoir recours à des prestations de services de Cloud computing. Ces recommandations indicatives sont principalement basées sur une analyse de risques réalisée au préalable par les clients et des engagements de transparence des prestataires vis-à-vis de leurs clients qui doivent être formalisés dans les contrats de prestation de services.

Recommandation n°1 : Identifier clairement les données et les traitements qui passeront dans le Cloud

Avant d'envisager le recours au Cloud computing, le client responsable de traitement doit clairement identifier les données, traitements ou services qui pourraient être hébergés dans le Cloud.

Pour chaque traitement, il doit établir quels types de données pourraient être concernés en distinguant :

- les données à caractère personnel,
- les données sensibles[1],
- les données stratégiques pour l'entreprise,
- les données utilisées dans les applications métiers.

Dans le cas où une partie seulement des données et traitements est transférée dans le Cloud, comme par exemple le logiciel de messagerie, le client doit veiller à s'assurer que les traitements passés dans le Cloud ne risquent pas d'inclure des données d'autres traitements qui n'ont pas migré. Un tel exemple est l'utilisation d'une messagerie « Cloud » dans laquelle les collaborateurs échangent des contenus stratégiques pour l'entreprise.

Par ailleurs, certains types de données sont soumis à une réglementation spécifique, il est donc nécessaire de vérifier si les données qui pourraient être transférées dans le Cloud sont soumises à de telles obligations et, lorsque cela est le cas, d'identifier les conditions minimales à leur transfert. Par exemple, les données de santé ne peuvent être stockées que par un hébergeur de données de santé agréé par le Ministère de la santé.

Recommandation n°2 : Définir ses propres exigences de sécurité technique et juridique

Le passage au Cloud demande une approche rigoureuse en termes de sécurité technique et juridique.

Contrairement aux offres classiques d'externalisation, dans lesquelles les prestataires fournissent une réponse personnalisée à un cahier des charges défini par le client, de nombreuses offres de Cloud sont « standard » pour tous les clients et ne répondent pas à un cahier des charges particulier.

Pour autant, le client doit définir ses propres exigences et évaluer si les offres envisagées répondent à l'ensemble des exigences formulées. En effet, si le but du Cloud est de décharger le client de certaines tâches opérationnelles, il doit s'assurer *a priori* que le prestataire suit un niveau d'exigence au moins égal au sien.

[1] Données sensibles au sens de l'article 8 de la Loi Informatique et Libertés ou données relevant de l'article 9.

Les exigences doivent comprendre l'ensemble des points importants pour le client et considérer notamment :

- les contraintes légales (localisation des données, garantie de sécurité et de confidentialité, réglementations spécifiques à certains types de données, etc.) ;
- les contraintes pratiques (disponibilité, réversibilité/portabilité[2], etc.) ;
- et les contraintes techniques (interopérabilité avec le système existant, etc.).

Pour les données et les traitements « métier », le client doit particulièrement veiller à garantir la réversibilité et s'assurer qu'un niveau de disponibilité suffisant est garanti par le prestataire et par son fournisseur d'accès à Internet.

Recommandation n°3 : Conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise

Conduire une analyse de risques complète est essentiel pour être en mesure de définir les mesures de sécurité appropriée à exiger du prestataire ou à mettre en œuvre au sein de l'entreprise. La méthode EBIOS[3] constitue une méthode pertinente pour l'analyse de risques à condition que les données à caractère personnel soient considérées dans les biens à protéger et que les impacts sur la vie privée des personnes concernées soient pris en compte.

Pour les organismes qui n'ont pas les moyens de mener une analyse complète, la Commission souhaite mettre en avant les risques suivants, qui sont plus importants dans le cas du Cloud que dans le cas de traitements informatiques traditionnels, et qui sont particulièrement pertinents pour la protection des données personnelles. Une liste plus complète de 35 risques fournie par l'ENISA[4] peut aussi être utilisée.

Les principaux risques identifiés par notre Commission sont les suivants :

- perte de gouvernance sur le traitement ;
- dépendance technologique vis-à-vis du fournisseur de Cloud Computing, c'est-à-dire l'impossibilité de changer de solution (pour un autre fournisseur ou une solution interne) sans perte de données ;
- faille dans l'isolation des données, c'est-à-dire le risque que les données hébergées sur un système virtualisé soient modifiées ou rendues accessibles à des tiers non autorisés, suite à une défaillance du prestataire ou à une mauvaise gestion du rôle d'hyperviseur ;

[2] La réversibilité (ou portabilité) est la possibilité de pouvoir obtenir une copie de l'intégralité de ses données dans un format structuré et couramment utilisé. Ceci permet au responsable de traitement de s'assurer qu'il puisse changer de solution si besoin sans perte d'information (données, structure, etc.).

[3] La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI.

[4] Agence Européenne chargée de la sécurité des réseaux et de l'information, rapport disponible en anglais et en espagnol à l'adresse suivante : http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

- réquisitions judiciaires, notamment par des autorités étrangères ;
- faille dans la chaîne de sous-traitance, dans le cas où le prestataire a lui-même fait appel à des tiers pour fournir le service ;
- destruction ineffective ou non sécurisée des données, ou durée de conservation trop longue ;
- problème de gestion des droits d'accès par les personnes causé par une insuffisance de moyens fournis par le prestataire ;
- indisponibilité du service du prestataire, ce qui comprend l'indisponibilité du service en lui-même mais aussi l'indisponibilité des moyens d'accès au service (notamment les problèmes réseaux) ;
- fermeture du service du prestataire ou acquisition du prestataire par un tiers ;
- non-conformité réglementaire, notamment sur les transferts internationaux.

Dans le cas où une partie seulement des données et traitements sont transférés dans le Cloud, comme par exemple le logiciel de messagerie, le client doit également considérer l'impact de la migration partielle sur les traitements et données non transférés, par exemple si les données sensibles ou stratégiques sont explicitement exclues du transfert dans le Cloud, les traitements nécessitant l'envoi de telles données par courriel devront être adaptés.

La plupart des ces risques ont vocation à être réduits par des dispositions contractuelles, pouvant inclure des pénalités pour le prestataire, et par des mesures techniques et organisationnelles au niveau du client et du prestataire. La Commission recommande que le client évalue la pertinence de ces risques pour sa propre situation et étudie les mesures mises en place par lui-même et par le prestataire pour réduire ces risques.

Recommandation n°4 : Identifier le type de Cloud pertinent pour le traitement envisagé

Il existe différentes offres de services de Cloud computing sur le marché, qui peuvent être distinguées selon trois modèles de services et trois modèles de déploiement.

Les modèles de services sont les suivants :

- SaaS : « Software as a Service », c'est-à-dire la fourniture de logiciel en ligne ;
- PaaS : « Platform as a Service », c'est-à-dire la fourniture d'une plateforme de développement d'applications en ligne ;
- IaaS : « Infrastructure as a Service », c'est-à-dire la fourniture d'infrastructures de calcul et de stockage en ligne.

Les modèles de déploiement sont les suivants :

- « Public » quand un service est partagé et mutualisé entre de nombreux clients ;
- « Privé » quand le Cloud est dédié à un client ;

- « Hybride » quand un service est partiellement dans un Cloud public et partiellement dans un Cloud privé. Dans ce cas, nous considérons que le service peut être étudié comme deux traitements interconnectés. Nous ne ferons donc pas référence à ce modèle de déploiement.

Chaque offre de service de Cloud computing étant spécifique, il convient de les comparer en identifiant les forces et les faiblesses de chacune au regard du traitement considéré. Une telle analyse permettra de sélectionner l'offre de Cloud computing la mieux adaptée.

Il est à noter qu'il peut tout à fait être envisagé de choisir des solutions de Cloud computing différentes en fonction des traitements. Ainsi, il est par exemple possible de choisir un service IaaS public français pour le site Internet de l'entreprise, un hébergeur de santé homologué pour les données de santé et un SaaS européen privé pour les courriels.

Non seulement une telle conception permet de choisir l'offre la plus adaptée à chaque traitement particulier, mais elle permet également de garantir une meilleure protection des données collectées par une entreprise puisqu'elles ne sont pas toutes confiées au même prestataire de services de Cloud computing.

Enfin, une approche par étape peut permettre une transition vers le Cloud computing progressive et ainsi de mieux appréhender les risques particuliers du Cloud computing. Il sera alors possible de tirer profit des premières expériences afin de faire évoluer les pratiques internes et de mieux négocier ou mieux choisir les contrats suivants.

Le transfert du traitement ou des données dans le Cloud peut ainsi s'effectuer progressivement par catégorie de données et exigence de sécurité croissante, par exemple en commençant par le transfert des logiciels support (messagerie, agenda, contacts, etc.), puis par les applications contenant des données sensibles ou stratégiques (par exemple les traitements RH) et en finissant par les applications métiers.

Recommandation n°5 : Choisir un prestataire présentant des garanties suffisantes

En tant que responsables du traitement, les clients de services de Cloud computing doivent s'assurer qu'ils sont en mesure de remplir leurs obligations. Pour ce faire, ils doivent choisir des prestataires garantissant la mise en place de mesures de sécurité et de confidentialité appropriées, et qui soient transparents vis-à-vis de leurs clients sur les moyens employés pour exécuter leurs prestations (transfert de données à l'étranger, recours à des sous-traitants, politique et mesures de sécurité, etc.).

Le choix d'un prestataire doit être effectué en considération de la grille d'analyse suivante :

Etape n°1 : Déterminer la qualification juridique du prestataire

Lorsqu'un client fait appel à un prestataire de services, il est généralement admis que le premier est responsable de traitement et le second sous-traitant.

Toutefois, la CNIL constate que dans certains cas de PaaS et de SaaS publics, les clients, bien que responsables du choix de leurs prestataires, ne peuvent pas réellement leur donner d'instructions et ne sont pas en mesure de contrôler l'effectivité des garanties de sécurité et de

confidentialité apportées par les prestataires. Cette absence d'instruction et de moyens de contrôle est due notamment à des offres standardisées, non modifiables par les clients, et à des contrats d'adhésion qui ne leur laissent aucune possibilité de négociation.

Dans de telles situations, le prestataire pourrait *a priori* être considéré comme conjointement responsable en vertu de la définition de « responsable du traitement » fournie à l'article 2 de la directive 95/46/CE, puisqu'il participe à la détermination des finalités et des moyens des traitements de données à caractère personnel.

Dans le cas d'une responsabilité conjointe, il est pertinent que les responsabilités incombant à chaque partie soient clairement définies.

La CNIL suggère alors le partage des responsabilités suivant :

Hypothèse	Formalités déclaratives	Information des personnes	Obligation de confidentialité et sécurité	Exercice des droits des personnes concernées auprès du …
Le prestataire est conjointement responsable du traitement	**Client**[5]	**Client**[6]	**Client + Prestataire**	**Client (avec le concours du prestataire)**[7]

Identifier si le prestataire est responsable conjoint du traitement ou non permet de déterminer qui est responsable vis-à-vis des autorités compétentes de protection des données personnelles.

En effet, en vertu des pouvoirs qui lui sont conférés par la loi Informatique et Libertés, la CNIL peut contrôler et sanctionner tout responsable du traitement qui ne respecterait pas ses obligations conformément à la loi Informatique et Libertés. Par conséquent, si le client et le prestataire sont conjointement responsables du traitement, ils seront tous deux susceptibles d'être contrôlés et potentiellement sanctionnés.

Etape n°2 : Evaluer le niveau de protection assuré par le prestataire aux données traitées

Quelle que soit la qualification du prestataire, il est de la responsabilité du client de choisir un prestataire qui assure un niveau de protection suffisant aux données qu'il lui confie.

La CNIL a listé ci-après les éléments essentiels, au regard de la protection des données personnelles, devant figurer dans un contrat de prestation de services de Cloud computing.

[5] Le client et le prestataire auront des obligations déclaratives auprès de la CNIL concernant le traitement dont ils sont conjointement responsables. Ils devront alors déterminer qui d'entre eux effectuera ces formalités. La CNIL recommande que ce soit le client qui s'en charge, puisque le recours à un prestataire de Cloud peut s'inscrire dans un traitement plus général, mais il est tout à fait envisageable que ce soit le prestataire qui s'acquitte des formalités pour son compte et pour celui du client. Dans tous les cas, la partie en charge de ces formalités déclaratives devra être en mesure de fournir la preuve, sur demande de l'autre partie, qu'elles ont été dûment effectuées auprès de la CNIL.

[6] Bien que l'obligation d'information incombe à la fois au client et au prestataire tous deux responsables de traitement, il est souhaitable qu'en pratique ce soit l'entité à laquelle la personne concernée a communiqué ses données qui l'informe des moyens de traitement auxquels le prestataire a recours. Par conséquent, le prestataire doit fournir au client toutes les informations nécessaires au respect de cette obligation d'information. Toutefois, le prestataire doit rester la personne de contact à laquelle la personne concernée devra s'adresser pour obtenir davantage d'information sur le traitement pour lequel le prestataire agit comme responsable conjoint du traitement.

[7] La dissémination possible des données sur différents serveurs localisés dans divers pays peut rendre plus compliqué l'exercice de leurs droits par les personnes concernées. Il convient alors de s'assurer que le prestataire et le client mettent en œuvre les garanties nécessaires pour permettre aux personnes concernées d'exercer leurs droits d'accès, de rectification, de modification, de mise à jour ou d'effacement.

Eléments essentiels devant figurer dans un contrat de prestation de services de Cloud computing

Informations relatives aux traitements

- Respect des principes européens en matière de protection des données personnelles et de la loi Informatique et Libertés (notamment des principes de proportionnalité et de respect des finalités) ;
- Existence d'un système de remontée des plaintes et des failles de sécurité ;
- Moyens de traitement ;
- Destinataires des données ;
- Sous-traitance :
  - Information et obtention du consentement du client en cas d'utilisation de tiers ou de sous-contractants situés ou non à l'étranger pour participer à la réalisation du traitement (Note : *si le prestataire est responsable conjoint du traitement, il devra seulement informer le client et non pas obtenir son consentement*) ;
  - Report dans les contrats de sous-traitance ultérieurs contractés par le prestataire des obligations contractuelles prévues dans le contrat de prestation signé entre le client et le prestataire et organisation de la responsabilité contractuelle des sous-contractants vis-à-vis du prestataire et du client.
- Existence de procédures simples permettant de respecter les droits des personnes concernées vis-à-vis de leurs données (droits d'accès, modification ou suppression, etc.).

Garanties mises en œuvre par le prestataire

- Durée de conservation des données limitée et raisonnable au regard des finalités pour lesquelles les données ont été collectées ;
- Destruction et/ou restitution des données en fin de prestation ou en cas de rupture anticipée du contrat dans un format structuré et couramment utilisé ;
- Devoir de coopération avec les autorités de protection des données compétentes ;
- Lorsque le prestataire est sous-traitant, indication que le client peut procéder à des audits du prestataire afin de s'assurer que ces garanties sont effectivement mises en œuvre.

Localisation et transferts

- Indication claire et exhaustive des pays hébergeant les centres de données du prestataire où les données seront traitées ;

- Assurance d'une protection adéquate à l'étranger (notamment grâce à des Clauses contractuelles types ou à des règles contraignantes d'entreprise « BCR ») ;

- Possibilité de limiter les transferts de données uniquement vers des pays membres de l'Espace Economique Européen ou vers des pays tiers reconnus comme assurant un niveau de protection adéquat par décision de la Commission européenne (*Note : Au contraire des autres éléments, celui-ci est laissé à la négociation des parties. En tout état de cause, un prestataire qui laisse la possibilité à ses clients de limiter les transferts de données vers des pays membres de l'EEE ou vers des pays tiers assurant un niveau de protection adéquat reconnu par la Commission européenne offrira à ses clients des garanties de protection des données renforcées. Toutefois, les clients doivent être conscients que lorsqu'ils choisissent des prestataires localisés dans des pays tiers, les autorités administratives ou judiciaires locales peuvent adresser des requêtes aux prestataires pour accéder aux données) ;*

- Information immédiate du client en cas de requête provenant d'une autorité administrative ou judiciaire étrangère.

Formalités auprès de la CNIL

- Lorsque le prestataire est sous-traitant, obligation de fournir au client toute information utile permettant de procéder à la déclaration du traitement auprès de la CNIL ;

- Lorsque le prestataire est responsable conjoint du traitement, le client et le prestataire doivent déterminer quelle partie sera en charge des formalités pour son compte et pour celui de l'autre partie. Quelle que soit la solution choisie, la partie qui ne déclare pas devra fournir à celle qui effectuera les formalités déclaratives toute information utile permettant de procéder à la déclaration du traitement auprès de la CNIL.

Sécurité et confidentialité

- Indication des obligations incombant au prestataire en matière de sécurité des données et, lorsque celui-ci est sous-traitant, précision qu'il ne peut agir que sur instruction du client ;

- Politique de sécurité et mesures minimales de sécurité :

[Note : le prestataire sous-traitant devra tenir à la disposition du client le détail des mesures mises en place, tandis que le prestataire responsable conjoint du traitement devra seulement garantir que des mesures suffisantes ont été mises en œuvre.]

  - Existence d'une politique de sécurité accessible ;

  - Mesures de sécurité et sûreté physique sur le site d'hébergement (protection du site et sécurité des accès, sécurité électrique et système de climatisation, etc.) ;

  - Mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données : par exemple, chiffrement des données et procédés garantissant ainsi que le prestataire n'a pas accès aux données qui lui sont confiées (chiffrement côté client, avec un algorithme reconnu et une gestion des clés adéquate, avant tout transfert) et liaison chiffrée avec le serveur de Cloud (connexion de type https ou VPN par exemple), etc. ;

  - Autres mesures de sécurité logique (protection du réseau (pare-feu, antivirus, détection d'intrusion, etc.), gestion des mises à jour, protection du terminal, gestion des habilitations, authentification des personnels, sécurité des développements applicatifs, etc.) ;

- Certifications : preuve de certifications pertinentes par des auditeurs indépendants et qualifiés, par exemple une certification ISO 27001 sur un périmètre incluant intégralement les services fournis, définition rigoureuse d'une politique d'audit du prestataire par le client comprise dans les garanties générales *[Note : au contraire des autres éléments, la certification est laissé à la négociation des parties. En tout état de cause, un prestataire qui dispose d'une certification offrira à ses clients des garanties de protection des données renforcées]* ;

- Réversibilité/portabilité : garantir la réversibilité ou la portabilité aisée des données dans un format structuré et couramment utilisé, sur demande du client et à tout moment ;

- Traçabilité : accès aux journaux de traçabilité des actions effectuées sur les données par les personnels du client et par ceux du prestataire et information de toute anomalie détectée par le prestataire ;

- Continuité de service, sauvegardes et intégrité : système de sauvegarde, redondance des serveurs, etc. ;

- Engagement de niveaux de services (« *Service Level Agreements* » ou « *SLAs* ») : engagements contraignants pour le prestataire sur le niveau de service, devant notamment prévoir des pénalités pour le prestataire en cas de non-respect des engagements contractuels. Ceci doit être mis en place en particulier pour les clauses relatives à la protection des données (durée de conservation, exercice des droits des personnes concernées, disponibilité du traitement, etc.).

Au vu de ces éléments essentiels identifiés par la CNIL, des modèles de clauses contractuelles pouvant être insérées dans les contrats de prestations de service sont proposés en annexe.

Ces modèles de clauses ont vocation à aider les sociétés clientes de services de Cloud, notamment les PME, à choisir un prestataire qui offre toutes les garanties nécessaires en termes de protection des données personnelles et de sécurité au regard de la loi Informatique et Libertés.

La CNIL rappelle que si ces éléments essentiels ne figurent pas directement ou indirectement dans un contrat de prestation, les clients ne seront pas en mesure de satisfaire aux obligations légales qui leur incombent en leur qualité de responsables de traitement.

Par conséquent, les prestataires qui n'offrent pas ces garanties essentielles dans leurs contrats et qui refusent toute négociation avec leurs clients potentiels ne devraient pas être sélectionnés. En effet, en acceptant de telles conditions contractuelles insuffisantes, les clients s'exposent à un risque élevé de non-conformité à la législation en vigueur.

En outre, lorsqu'il n'est pas possible de négocier un contrat de prestation de Cloud computing avec un prestataire, ces éléments essentiels doivent également servir de base aux clients pour comparer les différentes offres disponibles sur le marché et faire un choix pertinent qui tiendra compte de leurs obligations légales.

Recommandation n°6 : Revoir la politique de sécurité interne

Le Cloud computing suppose une révision complète des procédures internes conformément aux conclusions de l'analyse de risques. En effet, le recours au Cloud introduit de nouveaux risques liés en particulier aux transmissions par internet ou à l'utilisation de terminaux mobiles et nomades. Une attention particulière doit être apportée aux mécanismes d'authentification des employés et le prestataire de Cloud doit proposer un service compatible avec ces exigences de sécurité.

Recommandation n°7 : Surveiller les évolutions dans le temps

Dans un esprit d'amélioration continue, la Commission recommande de réaliser périodiquement une évaluation du service de Cloud computing en fonction de l'évolution dans le temps du contexte, des risques, des solutions disponibles sur le marché, de la législation, etc.

En particulier, la mise à jour de l'analyse de risques préconisée est nécessaire dès qu'une évolution significative du service a lieu afin d'adapter les mesures ou les solutions dès que nécessaire. Ces évolutions peuvent concerner les fonctionnalités du produit ou la fourniture technique du service (nouveau centre de données, changement de politique de sécurité, évolution du traitement initiée par le client, etc.).

DOCUMENT 4
Sécurité cloud : le guide des outils essentiels et des bonnes pratiques
***znet.fr* – 22 juillet 2021**

Sécurité : *Les applications dans le cloud se sont avérées essentielles pour permettre le travail à distance. Mais le cloud comporte ses propres risques de sécurité.*

Les services de cloud computing sont devenus un outil essentiel pour la plupart des entreprises. Cette tendance s'est accélérée récemment, les services dans le cloud tels que Zoom, Microsoft 365 et Google Workspace et bien d'autres devenant les outils de collaboration et de productivité de prédilection des équipes travaillant à distance.
Si le "cloud" est rapidement devenu un outil essentiel, son adoption peut également entraîner des risques supplémentaires en matière de cybersécurité.

Auparavant, la plupart des personnes qui se connectaient au réseau de l'entreprise le faisaient depuis leur lieu de travail et accédaient donc à leurs comptes, à leurs fichiers et aux serveurs de l'entreprise entre les quatre murs de l'immeuble de bureaux, protégés par des pare-feu et autres outils de sécurité de qualité professionnelle. Avec l'utilisation accrue des applications cloud, ce n'est soudainement plus le cas : les utilisateurs peuvent accéder aux applications, documents et services de l'entreprise depuis n'importe où. Cela a entraîné le besoin de nouveaux outils de sécurité.

Menaces liées au cloud

S'il est positif pour les travailleurs à distance - car il leur permet de continuer à travailler avec un semblant de normalité - le travail à distance représente également une opportunité pour les cybercriminels, qui ont rapidement profité du passage au travail à distance pour tenter de s'introduire dans les réseaux des organisations qui ont mal configuré leur sécurité cloud.

Les VPN d'entreprise et les suites d'applications dans le cloud sont devenus des cibles de choix pour les pirates. S'ils ne sont pas correctement sécurisés, tous ces éléments peuvent fournir aux cybercriminels un moyen simple d'accéder aux réseaux d'entreprise. Il suffit aux attaquants de s'emparer d'un nom d'utilisateur et d'un mot de passe, en les dérobant via un e-mail de phishing ou en utilisant des attaques par force brute pour pirater des mots de passe simples.
Comme l'intrus utilise les identifiants de connexion légitimes d'une personne travaillant déjà à distance, il est plus difficile de détecter un accès non autorisé, surtout si l'on considère que le passage au travail à distance a conduit certaines personnes à travailler à des heures différentes de celles que l'on pourrait considérer comme des heures de travail normales.

Les attaques contre les applications cloud peuvent être extrêmement préjudiciables pour les victimes, car les cybercriminels peuvent rester sur le réseau pendant des semaines ou des mois. Parfois, ils volent de grandes quantités d'informations sensibles sur l'entreprise ; parfois, ils utilisent les services cloud comme point d'entrée initial pour jeter les bases d'une attaque par ransomware qui peut les conduire à voler des données et à déployer un ransomware. C'est pourquoi il est important que les entreprises qui utilisent des applications cloud disposent des outils et des pratiques appropriés pour s'assurer que les utilisateurs puissent utiliser ces services en toute sécurité tout en étant capables de les utiliser efficacement.
Utiliser des contrôles d'authentification multi-facteurs sur les comptes d'utilisateurs.

Une mesure préventive évidente consiste à mettre en place des contrôles de sécurité solides sur la manière dont les utilisateurs se connectent aux services de cloud computing. Qu'il s'agisse d'un réseau privé virtuel (VPN, d'un service de protocole de bureau à distance (RDP) ou d'une suite d'applications bureautiques, le personnel doit avoir besoin de plus que son nom d'utilisateur et son mot de passe pour accéder à ces services.

"L'un des aspects les plus importants du cloud est que l'identité est reine. L'identité devient presque votre proxy pour absolument tout. Tout d'un coup, l'identité, son rôle et la façon dont vous l'attribuez ont tout le pouvoir", explique Christian Arndt, directeur de la cybersécurité chez PwC.

Qu'elle soit logicielle (l'utilisateur doit appuyer sur une alerte sur son smartphone) ou matérielle (l'utilisateur doit utiliser une clé USB sécurisée sur son ordinateur), l'authentification multifactorielle (MFA) constitue une ligne de défense efficace contre les tentatives d'accès non autorisées aux comptes. Selon Microsoft, la MFA protège contre 99,9 % des tentatives de connexion frauduleuses.
Non seulement elle empêche les utilisateurs non autorisés d'accéder aux comptes, mais la notification envoyée par le service, qui demande à l'utilisateur s'il a tenté de se connecter, peut servir d'alerte pour signaler que quelqu'un tente d'accéder au compte. Elle peut être utilisée pour avertir l'entreprise qu'elle pourrait être la cible de pirates informatiques malveillants.

Utiliser le chiffrement

La possibilité de stocker ou de transférer facilement des données est l'un des principaux avantages de l'utilisation d'applications cloud, mais pour les entreprises qui veulent garantir la sécurité de leurs données, leurs processus ne doivent pas se limiter à télécharger des données vers le cloud et à les oublier. Il existe une étape supplémentaire que les entreprises peuvent franchir pour protéger les données téléchargées vers les services de cloud computing : le chiffrement.

Tout comme lorsqu'elles sont stockées sur des PC et des serveurs ordinaires, le chiffrement des données les rend illisibles et les dissimule aux utilisateurs non autorisés ou malveillants. Certains fournisseurs de services cloud fournissent automatiquement ce service, en assurant une protection de bout en bout des données à destination et en provenance du cloud, ainsi qu'à l'intérieur de celui-ci, afin d'éviter qu'elles ne soient manipulées ou volées.

Appliquez les correctifs de sécurité le plus rapidement possible.

Comme d'autres applications, les applications cloud peuvent recevoir des mises à jour logicielles lorsque les fournisseurs développent et appliquent des correctifs pour que leurs produits fonctionnent mieux. Ces mises à jour peuvent également contenir des correctifs pour les vulnérabilités de sécurité, car ce n'est pas parce qu'une application est hébergée par un fournisseur de cloud computing qu'elle est invulnérable aux vulnérabilités de sécurité et aux cyberattaques.

Des correctifs de sécurité critiques pour les applications VPN et RDP ont été publiés par les fournisseurs afin de corriger les vulnérabilités de sécurité qui exposent les entreprises à des cyberattaques. Si ces correctifs ne sont pas appliqués assez

rapidement, les cybercriminels risquent d'abuser de ces services pour en faire un point d'entrée sur le réseau qui pourra être exploité pour d'autres cyberattaques.
Utilisez des outils pour savoir ce qui se trouve sur votre réseau.

Les entreprises utilisent de plus en plus de services cloud, et garder la trace de toutes les applications et de tous les serveurs qui ont été mis en service n'est pas une mince affaire. Mais il existe de très nombreux cas où les données d'entreprise sont exposées à cause d'une mauvaise utilisation de la sécurité du cloud. Un service cloud peut être laissé ouvert et exposé sans que l'entreprise le sache. Les ressources de stockage publiques exposées dans le cloud peuvent être découvertes par des attaquants, ce qui peut mettre toute l'entreprise en danger.
Dans ces circonstances, il peut être utile d'utiliser des outils de gestion de la posture de sécurité du cloud (CSPM). Ceux-ci peuvent aider les organisations à identifier et à répondre aux problèmes de sécurité potentiels liés à une mauvaise configuration dans le cloud, en fournissant un moyen de réduire la surface d'attaque que les pirates peuvent examiner, et en aidant à maintenir l'infrastructure du cloud sécurisée contre les attaques potentielles et les fuites de données.

"La gestion de la posture de sécurité dans le cloud est une technologie qui évalue la dérive de la configuration dans un environnement changeant, et vous alertera si les choses sont d'une manière ou d'une autre désynchronisées par rapport à ce qu'est votre ligne de base. Cela peut indiquer qu'il y a quelque chose dans le système qui peut être exploité à des fins de compromission", dit Merritt Maxim, vice-président et directeur de recherche chez Forrester.

La CSPM est une procédure automatisée et l'utilisation d'outils de gestion automatisés peut aider les équipes de sécurité à rester au fait des alertes et des évolutions. L'infrastructure du cloud peut être vaste et le fait de devoir passer manuellement au peigne fin les services pour trouver des erreurs et des anomalies serait trop lourd pour un humain - surtout s'il y a des dizaines de services de cloud différents sur le réseau. L'automatisation de ces processus peut donc contribuer à la sécurité de l'environnement cloud.

"Vous n'avez pas assez de personnes pour gérer 100 outils différents dans un environnement qui change tous les jours, donc je dirais qu'il faut essayer de se consolider sur des plateformes qui résolvent un gros problème et appliquer l'automatisation", déclare TJ Gonen, responsable de la sécurité du cloud chez Check Point Software, une société de cybersécurité.

Assurez-vous de la séparation des comptes administrateur et utilisateur.

Les services cloud peuvent être complexes et certains membres de l'équipe informatique auront un accès hautement privilégié au service pour aider à l'administrer. La compromission d'un compte administrateur de haut niveau pourrait donner à un attaquant un contrôle étendu sur le réseau et la possibilité d'effectuer toute action que les privilèges de l'administrateur autorisent, ce qui pourrait être extrêmement dommageable pour l'entreprise qui utilise les services de cloud computing.

Il est donc impératif que les comptes d'administrateur soient sécurisés par des outils tels que l'authentification multifactorielle et que les privilèges de niveau administrateur ne soient accordés qu'aux employés qui en ont besoin pour faire leur travail. Selon le

NCSC, les dispositifs de niveau administrateur ne doivent pas être en mesure de naviguer directement sur le web ou de lire les e-mails, car cela pourrait compromettre le compte.
Il est également important de s'assurer que les utilisateurs réguliers qui n'ont pas besoin de privilèges administrateur ne les possèdent pas, car en cas de compromission du compte, un attaquant pourrait rapidement exploiter cet accès pour prendre le contrôle des services cloud.

Utilisez les sauvegardes comme plan de secours.

Mais si les services cloud peuvent offrir des avantages aux organisations du monde entier, il est important de ne pas se reposer entièrement sur le cloud pour la sécurité. Si des outils tels que l'authentification à deux facteurs et les alertes automatiques peuvent contribuer à sécuriser les réseaux, aucun réseau n'est impossible à pénétrer, surtout si des mesures de sécurité supplémentaires n'ont pas été appliquées.

C'est pourquoi une bonne stratégie de sécurité du cloud doit également impliquer le stockage de sauvegardes des données et leur stockage hors ligne, de sorte qu'en cas d'événement rendant les services cloud indisponibles, l'entreprise dispose de quelque chose sur lequel travailler.
Utilisez des applications cloud simples à utiliser pour vos employés.

Il y a autre chose que les entreprises peuvent faire pour garantir la sécurité du cloud, et c'est de fournir à leurs employés les bons outils dès le départ. Les suites d'applications cloud peuvent faciliter la collaboration pour tout le monde, mais elles doivent aussi être accessibles et intuitives à utiliser, sinon les organisations courent le risque que les employés ne veuillent pas les utiliser.

Une entreprise pourrait mettre en place la suite d'applications cloud la plus sécurisée possible, mais si elle est trop difficile à utiliser, les employés, frustrés de ne pas pouvoir faire leur travail, pourraient se tourner vers des outils cloud publics à la place.
Ce problème pourrait conduire à ce que des données d'entreprise soient stockées sur des comptes personnels, créant ainsi un plus grand risque de vol, en particulier si un utilisateur ne dispose pas d'une authentification à deux facteurs ou d'autres contrôles en place pour protéger son compte personnel.

Le vol d'informations sur un compte personnel pourrait potentiellement conduire à une fuite de données étendue ou à une compromission plus large de l'organisation dans son ensemble.

DOCUMENT 5
Cloud souverain, trois niveaux sinon rien ?
– *aucœurdesmétiers.fr* – octobre 2019

Offrir un environnement cloud capable de répondre aux enjeux liés à la souveraineté est un point clé pour un grand nombre d'organisations aujourd'hui. Il faut dire que la donnée s'impose comme une source de valeur critique pour la compétitivité des entreprises et pour l'efficacité des organismes publics. La protection, la localisation et la confidentialité des données sont au centre du cloud souverain… qui pose aussi la question de leur degré de sensibilité et du principe de proportionnalité.

La France remet le pied dans les nuages

L'architecture d'un cloud souverain de l'Etat a pour objectif de renforcer sa souveraineté numérique et la maîtrise de ses données. Abandonné en 2015, le projet d'un cloud souverain a refait surface en 2018. Il repose sur la fourniture d'un service indépendant de droit français avec une localisation et un traitement des données en France. Il s'agit de proposer aux administrations, aux établissements publics et aux collectivités territoriales, un cloud digne de confiance, ouvert à des clouds externalisés. Les pouvoirs publics y voient un intérêt particulier pour accompagner et soutenir leur transformation digitale. Le but : héberger les données des citoyens dans un espace numérique sécurisé et pérenne en termes de stockage et de puissance de calcul, au travers d'une architecture open source.

Une fusée à trois étages

La France se dote donc d'une stratégie d'hébergement axée sur trois niveaux, selon le degré de sensibilité des données manipulées. Elle prévoit un« cloud externe », dans lequel figureront les données et les applications jugées peu sensibles. Un cloud intermédiaire, dit « cloud dédié », prévoit d'accueillir les renseignements et les outils de sensibilité moyenne. Enfin, un cloud dit « interne », doit abriter les données les plus sensibles, voire très sensibles. Ce dernier sera accessible à tous les ministères via un portail dédié et hébergé par l'administration, conformément aux exigences régaliennes de sécurité.

Critères de choix du stockage en ligne

Dans cet environnement à trois niveaux, chaque organisme public peut opter pour la formule qui lui convient le mieux. La question du « découpage » peut se poser alors. En effet, pourquoi ne pas stocker l'ensemble de ses données dans un cloud interne si celles-ci sont « seulement » à 80% considérées comme sensibles ? Dans ce domaine, qui peut le plus ne peut-il pas le moins ? Le choix dépend du niveau de sécurité des données requis mais aussi de leur typologie. La souveraineté et la conformité ne passent pas par une maîtrise totale des données, difficilement envisageable dans un contexte de globalisation des échanges. Néanmoins, elles reposent sur la capacité des organismes à cartographier, recenser et visualiser les points d'entrée et de traitement de leurs données. Autrement dit, sur une véritable stratégie « data-driven », à l'image de celle qui se déploie aujourd'hui dans les entreprises.

Un contexte réglementaire et économique favorable

Le contexte réglementaire et la maturité du marché créent des conditions favorables au déploiement d'un cloud souverain. L'entrée en vigueur en mai 2018 du Règlement européen de protection des données personnelles (RGPD) et de la directive européenne NIS (Network and Information Security) portant sur la sécurité des réseaux et des systèmes d'information, y sont pour beaucoup. Sans parler de la mise en place du volet cybersécurité de la Loi de Programmation Militaire pour les opérateurs d'importance vitale (dont la cybersécurité des SI est assurée par l'ANSSI*). Parallèlement, le cloud computing pèse de plus en plus lourd dans l'économie du numérique. Il devrait atteindre 411,4 milliards de dollars en 2020 (Gartner) tandis que le marché mondial des services de cloud public, lui, est estimé à 277 milliards de dollars en 2021, selon IDC.

DOCUMENT 6

Optimiser sa stratégie de sourcing cloud

***decisions-achats.fr* – avril 2018**

Avant de souscrire à un service cloud, mieux vaut prendre le temps de mettre en regard de ses propres besoins, les services et les conditions proposés par les différents prestataires cloud, tant en matière de coûts que de niveaux de services ou encore de sécurité des données.

Technologie au cœur des programmes de la transformation numérique de nombreuses sociétés, le cloud computing est peu à peu devenu une commodité répandue au sein des entreprises en France. Ses bénéfices ne sont plus à démontrer : réduction des coûts, accessibilité, élasticité, déploiement rapide de nouveaux services et applications, simplicité d'intégration, flexibilité, disponibilité du service, partage des données...

Avant-propos - Attention à ne pas commencer par se focaliser sur le choix du prestataire ! Il faut d'abord construire sa politique de sourcing, mener l'inventaire des services attendus, faire le tri entre ce qui doit être externalisé et ce qui doit rester en interne. Notre conseil : externaliser uniquement les services que vous maîtrisez déjà en interne ainsi vous garderez le contrôle en toute circonstance et vous vous assurerez de la réversibilité du service.

Aujourd'hui, il s'avère indispensable de se lancer dans le cloud et pour cela de bien préparer et budgétiser son projet afin de s'éviter toute déconvenue. Un tel projet étant susceptible de se révéler plus onéreux que prévu. Cet effet a été constaté par une étude menée en 2015 par le cabinet Vanson Bourne pour le compte de Sungard Availability Services, spécialiste de la continuité d'activités . S'il est aujourd'hui aisé et rapide de souscrire à un service cloud, mieux vaut prendre le temps de mettre en regard de ses propres besoins, les services et les conditions proposés par les différents prestataires cloud, tant en matière de coûts que de niveaux de services ou encore de sécurité des données.

Voici quelques points essentiels à vérifier avant de se lancer.

La réversibilité des données

Avant de confier ses données à un fournisseur Cloud, vérifiez en tout premier lieu les conditions de réversibilité. Le Cloud est et sera de plus en plus une commodité à acheter. L'entreprise agile doit pouvoir décider à tout moment et pour quelque raison que ce soit le changement de prestataire ou de service : le prestataire n'atteint pas les objectifs fixés ou ne respecte pas ses engagements ou bien l'entreprise a l'opportunité de bénéficier d'un nouveau/meilleur service chez un concurrent. Dans ce cas, le contrat doit stipuler les conditions de retour (préavis, coût, format de données, retour des données et suppression chez le fournisseur...) et intégrer des clauses de réversibilité partielle et totale.

Note sur les obligations légales d'audit, traçabilité et de conservation des données : dans le cas d'une réversibilité partielle ou totale avec archivage des données (changement d'applicatif), le fait de récupérer uniquement les données peut ne pas suffir aux services règlementaires (fiscaux notamment) qui demanderont à voir / auditer le processus informatique qui a produit ces données. Une historisation de l'applicatif en plus des données à la date d'archive peut s'avérer nécessaire.

La visibilité sur les services

L'entreprise a besoin d'avoir un pilotage précis des activités et services fournis par ses fournisseurs internes ou de solutions cloud. Lorsqu'une entreprise met en place une stratégie cloud (voir ci-dessus), c'est parce qu'elle souhaite souscrire aux services complémentaires (éventuellement chez des prestataires différents) à ceux qu'elle produit en interne. Il est nécessaire de disposer de tableaux de bord afin de suivre les activités sur chacun de ces services, et donc de s'outiller pour avoir une vision globale et aussi spécifique sur ces activités et services.

Note : l'outillage doit s'intégrer fluidement au SI interne et notamment à l'outil d'ITSM de supervision et consolidation de l'activité informatique et remonter au minimum des événements type "incidents". Ce point qui semble évident représente un projet conséquent d'interfaçage.

DOCUMENT 7

Pourquoi les collectivités doivent s'intéresser au cloud souverain

zdnet.fr - 18 juin 2021

Technologie : *Alors que le Gouvernement vient de dévoiler sa stratégie nationale pour le cloud, les collectivités locales ont toutes les bonnes raisons de s'intéresser à la notion de cloud souverain explique Laurent Cervoni, de Talan*

Avec la crise sanitaire qui a rappelé notre dépendance aux nouvelles technologies étrangères pour notamment organiser le télétravail, la souveraineté numérique est devenue un enjeu majeur. Depuis le début de l'année, l'Etat s'est positionné sur les domaines clés où la France doit recouvrir sa pleine souveraineté. En janvier, l'Elysée présentait ainsi son plan stratégique sur la recherche quantique et, le mois suivant, la stratégie nationale en matière de cybersécurité.
Il y a quelques semaines, Talan présentait son livre blanc sur la souveraineté de la donnée et les enjeux d'un cloud européen.

Le 17 mai, c'était au tour du Gouvernement d'annoncer sa stratégie nationale pour le cloud. Un label "cloud de confiance" permettra aux entreprises et administrations françaises de bénéficier des services offerts par le cloud tout en assurant la meilleure protection pour leurs données.

Autre pilier du plan, la politique dit "Cloud au centre" visant à accélérer la transformation numérique du service public. "Chaque produit numérique manipulant des données sensibles" devra être hébergé sur le cloud interne de l'Etat ou sur un cloud industriel certifié par l'Anssi (Agence nationale de la sécurité des systèmes d'information).

Le spectre du Cloud Act

Au-delà de ce nouvel impératif, les collectivités locales ont de nombreuses bonnes raisons de s'intéresser à la notion de cloud souverain.

"Dura lex sed lex", la première est d'ordre réglementaire. Comme le rappelle une circulaire datant d'avril 2016 (5), signée par les ministres de l'Intérieur et de la Culture et de la Communication de l'époque, tout document produit par une collectivité est considéré, au regard du Code du patrimoine, comme une archive publique, donc un trésor national qui ne doit pas quitter nos frontières.

Des collectivités qui transmettaient les documents relatifs aux délibérations sur des services de stockage en ligne d'origine étrangère comme Dropbox, Google Drive ou WeTransfer ont ainsi adopté des solutions made in France comme hubiC d'OVHcloud ou Docapost-Fast du groupe La Poste.

Cette injonction réglementaire a aussi incité les cloud providers américains et en particulier Microsoft Azure et Amazon Web Services à implanter des datacenters en France. Ces hyperscalers restent toutefois soumis au Cloud Act qui, comme le Patriot Act avant lui, introduit le principe d'extraterritorialité.

Promulgué quasi en même temps que le RGPD, ce Clarifying Lawful Overseas Use of Data Act contraint les fournisseurs américains à divulguer des informations

personnelles sur leurs utilisateurs dans le cadre d'enquêtes judiciaires, même si les données ne sont pas hébergées sur le sol américain. Il y a donc un risque potentiel que des données nationales soient exportées sur demande d’un juge américain.

Des champions du cloud français

Au-delà de ce cadre légal, retenir un hébergement local favorise l'emploi sur le sol national. Dans le domaine du cloud, la France a la chance de disposer de belles pépites avec OVHcloud, premier hébergeur européen, 3DS Outscale, filiale de Dassault Systèmes, Scaleway, Aquaray ou encore Oodrive.

Certains d'entre eux sont certifiés SecNumCloud, le référentiel de bonnes pratiques de l'Anssi en matière de sécurité. Il vise à accroître la protection des administrations ou des OIV (Opérateurs d’Importance Vitale) en édictant un certain nombre d'exigences en termes d'authentification, de chiffrement ou d'hébergement en France.

Dans le cadre d'une stratégie de numérique responsable, faire appel à un hébergement permet, par ailleurs, de réduire l'empreinte carbone des services cloud. Un rapport d'information du Sénat plaide ainsi pour une relocalisation des datacenters. Malgré la meilleure optimisation de l'efficience énergétique des hyper datacenters des GAFA, "les émissions associées à l’utilisation (57 %) sont légèrement plus élevées à l’étranger (30 %) qu’en France (27 %).

Enfin, le cloud peut constituer une planche de salut pour les collectivités locales et territoriales qui ont une myriade d'applications métiers pour gérer la voirie, le cadastre, l'état civil ou les cantines scolaires. Le recours au mode SaaS permet, à ces administrations aux ressources informatiques limitées, de s'affranchir de la maintenance des infrastructures et de l'évolutivité des solutions en confiant ces tâches à des éditeurs de proximité et de confiance.

Ces spécialistes offrent, par ailleurs, toutes les garanties en matière de protection des données personnelles, conformément aux exigences du RGPD. Les collectivités n'ont pas vocation à gérer leurs propres datacenters. On les attend sur bien d'autres terrains.

Ainsi, le cloud est au cœur des enjeux de transformation des collectivités. A l’heure où la défiance des citoyens est de plus en plus importante envers les institutions, le cloud peut permettre aux collectivités de contribuer à bâtir un monde plus (éco)responsable, plus collaboratif et où chaque citoyen sait que ses données restent sous son contrôle. A condition de se saisir du cloud au plus vite.

DOCUMENT 8

Les collectivités pourront récupérer la TVA sur les services IaaS

***solutions-numeriques.com* - 28 juillet 2020**

Les députés français ont rendu éligible au fonds de compensation de la TVA (FCTVA) les dépenses en services d'infrastructure IT dans le Cloud (Iaas) des collectivités locales. Même limité à 5,6%, le dispositif corrige une distorsion de concurrence entre les achats IT sur site et dans le Cloud.

La loi votée en juillet 2020 est une très bonne nouvelle pour les hébergeurs, les fournisseurs et les revendeurs de services Cloud français, comme étrangers. Mais attention, elle ne concerne que les achats de service d'Infrastructure vendus comme un Service (IaaS). Ils seront éligibles dès le 1er janvier 2021 à un taux de compensation forfaitaire, limité volontairement à 5,6%, afin de ne pas créer trop de charge pour l'État.

Le nouveau dispositif corrige partiellement une distorsion de concurrence entre les achats informatiques traditionnels sur site et ceux dans le Cloud chez les collectivités locales. Cette recommandation figurait dans le rapport « *Faire de la France la première Nation Cloud* » remis dès 2017 au Gouvernement par l'association EuroCloud France.

Accélérer le développement des services Iaas dans les collectivités

Le vote de cette loi par les députés français en juillet 2020 permettra d'accélérer le développement des services Iaas dans les collectivités locales et territoriales. Jusqu'à présent, elles hésitaient à acheter des services dans le Cloud, souvent facturables sous forme d'abonnement (Opex), car ces mairies ou autres administrations locales ne peuvent récupérer la TVA que sur des produits achetés en mode Capex. Et comme il n'y a donc pas non plus d'enrichissement du patrimoine de la collectivité, leurs achats Cloud n'étaient pas éligibles à une compensation de la TVA via le fonds de compensation pour la taxe sur la valeur ajoutée (FCTVA).

Le FCTVA ne finançait que les dépenses d'investissement non récurrentes

En effet, le FCTVA permet à la base le remboursement intégral de la TVA acquittée par les collectivités territoriales et leurs groupements sur leurs dépenses réelles d'investissement. Auparavant, les seules dépenses d'investissement éligibles étaient celles non récurrentes visant à l'achat d'un équipement comptabilisé dans le patrimoine de la collectivité. Elles concernaient également les dépenses d'amélioration ou de réparation destinées à augmenter la valeur d'un bien déjà acquis.

Le Gouvernement n'était pas favorable à cette mesure en avril

Le passage de cette loi sur la TVA en faveur des services laas n'était pas gagné d'avance. En avril 2020, le Gouvernement n'était pas favorable au fait de faire bénéficier les collectivités territoriales et leurs groupements des attributions du FCTVA pour les dépenses informatiques liées au Cloud. Il a changé d'avis en juillet lors du vote de son troisième Projet de Loi de Finances rectificatif (PLFR3).

Grâce notamment aux députés Nicolas Forissier et Eric Bothorel, qui avaient invité dès avril le Gouvernement, via des amendements au premier Projet de Loi de Finance 2020, à mettre en adéquation sa volonté d'inciter les collectivités à avoir recours au Cloud, dans le cadre de la numérisation des services de l'État et de sa politique fiscale.

Le Gouvernement avait alors refusé, estimant que les services Cloud représentent des dépenses de fonctionnement qui ne correspondent pas à l'objectif du FCTVA, qui vise à soutenir l'investissement local. En outre, ils compliqueraient l'automatisation du FCTVA déjà reportée en 2021.

Rappelons que, dans le même registre, la Loi de Finance 2020 a modifié l'article L. 1615-1 du code général des collectivités territoriales afin d'étendre le bénéfice du FCTVA aux dépenses d'entretien des réseaux payées à compter du 1er janvier 2020.

DOCUMENT 9

Le cloud computing, dissipons les nuages
lagazettedescommunes.com - avril 2019

Le gouvernement a présenté une stratégie dédiée au cloud computing pour les organisations publiques. Tous les freins à l'équipement sont-ils levés ?

Le gouvernement a présenté le 3 juillet 2018 sa stratégie afin de favoriser l'adoption du cloud computing par les organisations publiques. Réparti en trois cercles (interne, dédié et externe, le cloud constitue une réelle opportunité pour moderniser les systèmes d'information, et au-delà, le service public offert aux usagers.

De nombreuses organisations publiques ont déjà adopté des solutions en mode SaaS (*software as a service* : utilisation d'applicatifs externalisés chez un éditeur), moins fréquemment en IaaS (*Infrastructure as a Service*), plus rarement en PaaS (*Platform as a Service*).

On constate que le plus souvent, elles privilégient un paiement de ces services basé sur un mode de redevance fixe, quel que soit le niveau réel des consommations. Or, l'une des innovations du cloud consiste à basculer vers un modèle de paiement à l'usage (*pay per use*). Ce qui nécessitera de la part des organisations publiques un arbitrage constant entre services externalisés (*on cloud*) et utilisation des capacités installées (*on premise*). Cet arbitrage sera rendu sur la base de critères techniques et financiers.

Souveraineté et protection des données

La domiciliation des données sur le territoire européen, voire français, est souvent présentée comme un frein à la généralisation du cloud computing. Il faut modérer cet argument. Plusieurs cloud services providers (CSP) sont basés en Europe, quelques-uns en France : ils échappent ainsi aux contraintes du Patriot Act américain.

Par ailleurs, les technologies de cryptage et de clés privatives renforcent les dispositifs de protection des données. Les certifications de l'ANSSI garantissent un haut niveau de protection des données. Enfin, les « trois cercles » de la stratégie cloud vont dans le sens de la souveraineté et la protection des données, tout en tenant compte de la réalité de l'offre technologique « cloud » du marché.

Les débats sur un cloud souverain sont donc derrière nous. Le risque de fuite de données ou de hacking réside bien plus souvent dans le manque de vigilance de l'utilisateur (session restée ouverte, mots de passe inchangés, installation de logiciels non agréés par le RSSI…) et les lacunes des dispositifs de cyber-protection.

Le cloud computing, en particulier le recours à des applications en mode SaaS, est parfois accusé favoriser le développement du *shadow IT*, et ainsi « d'échapper » aux DSI. Le risque est réel : il est indispensable que ces dernières soient motrices, aux côtés des Métiers, pour piloter le déploiement des solutions cloud. Que ce soit les modalités de migration du parc applicatif (legacy versus nouvelles applications), le développement d'API, l'interopérabilité des solutions cloud aux suites logicielles existantes ou encore les conditions de portabilité, la DSI doit jouer pleinement son rôle de conseil auprès des directions générales.

Dépenses d'investissement, ou de fonctionnement ?

Le véritable changement pour les DSI résidera dans leur service Exploitation, dont les effectifs seront revus à la baisse et les missions, pour une part, externalisées chez le CSP. Elles doivent également se préparer à l'exercice de nouveaux métiers de pilotage des infrastructures cloud, y compris sur la maîtrise financière et économique du recours au cloud (FinOp's). : le paiement à l'usage nécessite de repenser complètement les modalités d'achats et de contrôle des engagements. Pas si simple pour les acteurs publics ! A ce sujet, considérer ces dépenses comme de l'investissement, et non du fonctionnement, serait de nature à généraliser le recours aux technologies cloud.

La bascule vers le modèle cloud est inéluctable. C'est un des éléments de l'agilité dont les SI ont besoin : réduction des délais projet, réduction des charges de réseau, amélioration de l'accès des usagers aux services, diminution des coûts. Mais, l'acquisition de technologies en nuage diffère de la plupart des acquisitions de technologies traditionnelles connues du secteur public. Alors oui, avant toute décision d'achat, une phase d'appropriation préalable sera nécessaire.

DOCUMENT 10

Une limitation de l'éligibilité au FCTVA des dépenses de cloud engagées par les collectivités ?

***lagazettedescommunes.com* - 26 octobre 2021**

Réponse du ministère chargé des Comptes publics : L'article 69 de la loi n° 2020-955 du 30 juillet 2020 de finances rectificative a élargi l'éligibilité au FCTVA pour les dépenses d'informatique en nuage ou cloud.

Cet article dispose qu'est éligible au FCTVA la fourniture de prestations de solutions relevant de l'informatique en nuage déterminées par un arrêté conjoint du ministre chargé des finances, du ministre chargé des relations avec les collectivités territoriales et du ministre chargé du numérique payées à compter du 1er janvier 2021.

L'arrêté du 17 décembre 2020 fixe précisément la définition des dépenses éligibles.

Conformément à la volonté du législateur, l'éligibilité est effectivement limitée aux seules prestations d'informatique en nuage ou cloud de type infrastructure en tant que service (infrastructure as a service – iaas) afin d'éviter les effets d'aubaine, certaines collectivités recourant déjà antérieurement à des services de type plateforme en tant que service (platform as a service – paas) ou logiciel en tant que service (software as a Service – saas).

Par conséquent si les collectivités restent libres de retenir les solutions les plus adaptées à leurs besoins, les règles d'attributions du FCTVA permettent de soutenir les collectivités qui souhaitent migrer des systèmes traditionnels vers des solutions d'informatique en nuage de type infrastructure en tant que service (iaas).

Références :
Question écrite de Jean-Christophe Lagarde, n°33293, JO de l'Assemblée nationale du 22 juin 2021.

DOCUMENT 11
Le paradoxe du cloud : réduire les coûts, mais dépenser plus
***itforbusiness.fr* - 8 mars 2018**

Une étude montre que l'objectif de réduction des coûts souvent mis en avant pour l'adoption du cloud se termine en réalité par une augmentation des dépenses dans les infrastructures cloud. La faute à un afflux de consommation et de mauvaise gestion des services cloud.

451 Research a mené une étude sur l'adoption du cloud avec un focus sur les coûts de cette migration. Le cabinet précise dans son introduction que la stratégie cloud ne se décide pas du jour au lendemain et que la réflexion des entreprises porte sur des besoins métiers : transformation digitale, consolidation du SI, applications en mode SaaS, etc. Mais derrière cette analyse, la notion de coût est toujours sous-jacente. La réduction des coûts est même citée par près de 40% des responsables informatiques. La capacité d'allouer des ressources en fonction de la demande, l'agilité pour le time to market, amélioration de la disponibilité et réduction de management interne, sont les autres éléments de décision.

Selon l'analyse, « *la réalité ne correspond pas aux attentes* ». Certes, la plupart des entreprises réalisent des économies immédiates après la migration des charges de travail vers le cloud. Cependant, ces économies initiales sont érodées par les « *coûts de transformation* » correspondant aux coûts de migration des applications. Dans le meilleur des cas, ces coûts sont maîtrisés en nécessitant seulement quelques jours-hommes, mais d'autres cas impliquent de ré-architecturer, voire de reconstruire les applications. Et là, les coûts explosent. Dans le même temps, les coûts d'infrastructures augmentent lentement et sûrement, rappelle l'étude. On pense notamment au stockage et au réseau, souvent oubliés dans la facture finale.

Le paradoxe de Jevons appliqué au cloud

La migration passée, plus de la moitié des DSI considère que le point de tension réside dans le coût du cloud. Pour expliquer ce sentiment, 451 Research parle du « *paradoxe de Jevons* ». Prenant le nom de l'économiste britannique William Stanley Jevons, ce paradoxe énonce qu'à mesure que les améliorations technologiques augmentent l'efficacité avec laquelle une ressource est employée, la consommation totale de cette ressource peut augmenter au lieu de diminuer.

Adapté au cloud, cela signifie que comme le cloud est une technologie peu coûteuse et facilement accessible, les utilisateurs sont incités à consommer plus. Conséquence, si les coûts unitaires restent bas, les coûts globaux augmentent.

Gouvernance des ressources et management des déchets

Pour éviter les dérapages budgétaires, les entreprises peuvent décider à l'extrême de réinternaliser certains workload dans leurs datacenters. Un cas assez limité, constate le rapport. L'option la plus choisie est la mise en place de règles de gouvernance sur les ressources cloud en priorisant la consommation en fonction des projets ou en déléguant la maîtrise des coûts aux départements métiers. Dans ces cas-là, une majorité de sociétés se sert d'outils tiers pour endiguer les dépenses.

En complément de la question de la gouvernance, Research 451 pointe la question des « déchets » du cloud. En devenant une informatique « utilitaire et flexible », les utilisateurs consomment de la ressource informatique, mais oublient parfois d'arrêter les VM créées, les surdimensionnent ou elles ne correspondent plus à la nature du projet. Bref, la consommation appelle la surconsommation et donc le surcoût.

DOCUMENT 12

La cybersécurité des entreprises –
Prévenir et guérir : quels remèdes contre les cyber virus ?
extrait - *senat.fr* - 21 juin 2021

UN RECOURS CROISSANT AU CLOUD

1. Un remède à l'insuffisance des ressources internes de cybersécurité : l'infogérance

En France, en 2016, 17 % des sociétés de 10 salariés ou plus avaient acheté des services de *cloud computing* contre 12 % en 2014 selon l'INSEE. La tendance s'est depuis accentuée puisque selon Eurostat, les activités liées à la sécurité des TIC étaient réalisées par des **fournisseurs externes dans les deux tiers** des entreprises européennes. Cette proportion est identique pour les PME.
La sécurisation des données peut inclure le chiffrement de bout en bout (*encryption end-to-end*), la microsegmentation (technique de sécurité des réseaux qui permet aux architectes de la sécurité de diviser logiquement le centre de données en segments de sécurité distincts) ou encore la mise en place d'un réseau privé virtuel (VPN - *Virtual Private Network*).

L'infogérance est cependant toujours un risque comme le souligne dès décembre 2010 l'ANSSI, dans un guide sur l'externalisation des systèmes d'information et notamment d'une messagerie d'entreprise ou d'une suite bureautique auprès d'un prestataire d'informatique en nuage : « *les informations échangées ou traitées par ce biais (pièces jointes, agendas des décideurs, etc.) peuvent revêtir un caractère «sensible», et sont susceptibles d'intéresser la concurrence (intelligence économique)* », en recommandant, « *en l'absence de cadre juridique international adapté à l'informatique en nuage* », « *de s'assurer que les données à caractère personnel restent localisées sur des serveurs exclusivement situés dans l'Union européenne - voire en France - et de prévoir les moyens de contrôle de cette obligation* », ce que l'évolution de l'économie numérique n'a pas permis d'assurer.

Un **Plan d'Assurance Sécurité** (PAS) précise la liste exhaustive des équipements et des programmes concernés par la maintenance informatique ainsi que l'assistance sur site et la récupération des données en fin de contrat, y compris celles confiées à des sous-traitants (clause de réversibilité). Ces derniers sont qualifiés par l'ANSSI comme « *le maillon faible de la chaîne de cybersécurité* », dont le recours doit être encadré.

Mettant en exergue le fait que « *passer au cloud, c'est entamer une transformation numérique favorisant la croissance de l'entreprise* », le site public FranceNum, portail de la transformation numérique des entreprises, renvoie au dossier du 11 février 2019 du magazine Capital.fr : pourquoi le cloud devient un passage obligé pour les entreprises ?
Cependant, les PME, et plus encore les TPE, n'ont toujours pas les ressources pour réaliser un tel plan.

2. Un déséquilibre des relations contractuelles dans le cloud au détriment des PME

La cybersécurité dans le cloud diffère juridiquement et économiquement de l'acquisition d'un logiciel. L'acquisition d'un bien matériel de cybersécurité (logiciels) bénéficie de la garantie légale de conformité (article L.217-1 du code de la consommation), de la garantie légale des vices cachés (article 1641 du code civil) ou de la responsabilité du fait des produits défectueux. Son acquisition, sa maintenance en infogérance, relèvent du droit classique des relations contractuelles, faisant l'objet d'une abondante jurisprudence, et semble constitutive d'une relation équilibrée entre clients et fournisseurs.

En revanche, lorsqu'elles sont hébergées dans des plateformes appartenant à des GAFAM, les PME souffrent d'un déséquilibre des relations contractuelles.
Selon Eurostat, **14 % des entreprises européennes sont fortement dépendantes du *cloud* pour leur activité**, et celles-ci sont mal équipées pour faire face à la puissance monopolistique des fournisseurs de solutions de *cloud computing*. Cette situation est particulièrement vraie pour les PME : « *si 72 % des PME interrogées déclarent avoir l'intention d'en changer, 57 % déclarent avoir des difficultés à la faire. Cet effet de lock-in est lié à un manque de portabilité des données et de transférabilité, et heurte la capacité des organisations à choisir librement leur prestataire de service* », selon la Plateforme RSE.

Cette situation perdure malgré le **principe de libre circulation des données** établie par la Stratégie pour un Marché unique numérique lancée en mai 2015, déclinée par le règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, et les lignes directrices du 29 mai 2019 qui « *encourage les acteurs du secteur à élaborer, avec le soutien de la Commission, des codes de conduite fondés sur l'autorégulation concernant le changement de fournisseurs de services et le partage des données ».*

Des codes de conduite devaient être rédigés par les parties prenantes, l'un pour le marché du IaaS (*Infratructure As A Service*) et l'autre pour le marché du SaaS (*Software As A Service*), par le « SWIPO Working Group » (SWItching cloud and POrting data), mis en place en avril 2018 et devaient être présentés en novembre 2019 mais aucun consensus n'a pu être trouvé. Le CIGREF a donc publié le **26 mai 2021** un **référentiel du cloud de confiance**. Ce référentiel opérationnel a vocation à être également contractuellement exigible. Il n'est ni un label ni une certification.
Ce **coup d'arrêt du processus d'autorégulation du marché du cloud en Europe** est, pour le CIGREF, « *la conséquence d'une **asymétrie systémique** de compétences, de moyens et d'objectifs de certains grands fournisseurs mondiaux de services cloud d'une part, qui défendent le coeur de leur activité commerciale et leur capacité d'enfermement de leurs clients, et d'autre part ceux des utilisateurs dont le lobbying dans ce domaine n'est pas le métier* ». Les principaux fournisseurs ont refusé d'intégrer les attentes des utilisateurs en matière de régulation du cloud, notamment en termes d'interopérabilité logicielle et de portabilité des licences logicielles.

Pour une TPE ou une PME, la relation dans le cloud est déséquilibrée en faveur des fournisseurs. Si la contractualisation entre les PME et les opérateurs du *cloud* permet d'obtenir des garanties opérationnelles et de sécurité, les PME ne peuvent maitriser suffisamment cette évolution en raison de l'asymétrie des positions des acteurs de ce marché qui leur donne **un faible pouvoir de négociation.** Or, « *la décision de recourir au cloud n'est ni facilement réversible ni clairement neutre. Elle résulte d'une obligation opérationnelle de minimisation des coûts* » estime la Plateforme RSE dans son rapport précité. Un rapport du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies de juin 2020 confirme cette asymétrie.

Faute de contentieux (les différends ne se règlent pas devant la justice mais par transaction) mais en se fondant sur un rapport au Parlement européen qui soulignait qu'« *une comparaison de quatre contrats pour des services d'informatique en nuage destinés au grand public révèle que les fournisseurs **déclinent toute responsabilité** en matière de disponibilité ou de fonctionnalité du service, et qu'ils **se prémunissent contre les éventuels dommages causés aux consommateurs*** », la mission a dressé le même constat en juin 2020 pour les contrats cloud destinés aux professionnels. **Une telle apathie est surprenante alors que les cyberattaques dans le cloud n'ont cessé de croître**.

Certes, les dispositions existantes, qu'il s'agisse du code civil, du code de la consommation ou du code de commerce, pourraient être invoquées par les entreprises lésées. Or, **elles ne le sont pas**. Les **actions** engagées **en justice** sont le fait d'associations de consommateurs ou de la DGCCRF, notamment pour faire condamner (par l'Autorité de la concurrence) les GAFAM. Les entreprises préfèrent la discrétion de la transaction, et s'abstenir d'attraire leur fournisseur de cybersécurité en ligne devant la justice.

DOCUMENT 13

Le gouvernement adopte le cloud pour un stockage ultra-sécurisé des données

***weka.fr* - 9 juin 2021**

Le gouvernement a annoncé le 17 mai 2021 que le cloud devient désormais le mode d'hébergement par défaut des services numériques de l'État. Cette stratégie repose notamment sur la création du label SecNumCloud, qui certifiera les services des fournisseurs, avec un niveau de protection technique et juridique des données parmi les plus élevées au monde.

Désormais, les services numériques de l'État seront hébergés par défaut sur le cloud : c'est la doctrine dite « cloud au centre », que le gouvernement a présentée le 17 mai 2021. Elle concernera les nouveaux produits numériques et ceux qui connaissent une évolution substantielle. Car, si les technologies d'informatique « en nuage », qui permettent d'héberger et de traiter toujours davantage de données, seront un support essentiel aux innovations dans de nombreux secteurs, ce marché est dominé par des acteurs internationaux, américains notamment, parfois soumis à des lois à portée extraterritoriale qui les autorisent à accéder aux données stockées. Hors de question d'exposer les données françaises, des citoyens, des administrations et des entreprises, à un risque de transfert hors de l'Union européenne, estime le gouvernement.

« Le cloud permet de développer de nouveaux services publics numériques de manière plus rapide, plus agile, moins coûteuse et plus itérative », a constaté Amélie de Montchalin, ministre de la Transformation et de la fonction publiques. Les services numériques des administrations seront hébergés sur l'un des deux clouds interministériels internes de l'État ou sur les offres de cloud proposées par les industriels, à condition de satisfaire à des critères de sécurité stricts. Chaque service numérique traitant d'informations sensibles (données personnelles des citoyens, données économiques des entreprises, applications métiers relatives aux agents de l'État) devra impérativement être hébergé sur le cloud interne de l'État ou sur un cloud industriel ayant obtenu la qualification SecNumCloud de l'Anssi* (trois entreprises déjà labellisées) et protégé contre toute réglementation extracommunautaire. Le label offrira une sécurisation juridique et technique qui permettra aux administrations et aux entreprises de bénéficier des meilleurs services cloud au monde. Ils pourront être labellisés sous certaines conditions : entité opérant les services, localisation des données, exigences de sécurité, portages opérationnel et commercial par une entité européenne….

À partir du moment où les offres de confiance seront disponibles, les ministères auront douze mois pour mettre leurs projets en conformité et supprimer ainsi tout risque de transférer des données en dehors du territoire de l'Union européenne. « Nous allons également rendre réellement interministériels les clouds internes de l'État pour éviter, comme c'était le cas aujourd'hui, que chaque ministère poursuive la construction de ses propres infrastructures », a précisé Cédric O, secrétaire d'État chargé de la transition numérique et des communications électroniques.

L'usage du cloud renforcera la continuité du service public des produits numériques des administrations, qui s'appuieront sur une diversité de technologies, de fournisseurs et d'infrastructures, et qui prépareront des plans de continuité et de reprise d'activité, à activer en cas d'incident. Les agents seront équipés d'outils de travail plus collaboratifs, et les démarches des usagers en ligne seront améliorées. Ainsi, Amélie de Montchalin a expliqué que le gouvernement attend des agents qu'ils puissent « produire les meilleurs résultats en termes d'innovation, de transformation et en utilisant au mieux les compétences et l'engagement qui est le leur au service de ce numérique de qualité {…} et qu'ils puissent s'appuyer sur les solutions numériques de pointe » (partage de documents collaboratif, visioconférence…).

À noter que les recrutements et les programmes de formation continue destinés aux 18 000 agents publics de la filière numérique comporteront un volet cloud. Par ailleurs, au-delà de l'État, toute la sphère publique peut être concernée par cette nouvelle stratégie, pour basculer également ses investissements et ses pratiques informatiques, notamment les collectivités, comme l'a rappelé le directeur interministériel du numérique, Nadi Bou Hanna.

DOCUMENT 14
Loi n°2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France (REEN)
***kiosque.bercy.gouv.fr* - 15 novembre 2021**

Durant le premier semestre 2020, la mission d'information sur l'empreinte environnementale du numérique constituée au sein de la commission de l'aménagement du territoire et du développement durable du Sénat a mené un vaste cycle d'auditions qui a permis de recueillir les témoignages des principaux acteurs français et étrangers du secteur.

Ce travail a permis la publication d'un rapport dressant un état des lieux de l'empreinte environnementale du numérique en France, évaluant son évolution dans les prochaines années et formulant des pistes d'action pour les politiques publiques concernées. L'objectif de ces investigations était de pouvoir engager la France dans une transition numérique compatible avec les objectifs de l'Accord de Paris de lutte contre le réchauffement climatique.

Ces travaux se sont concrétisés par le dépôt de la proposition de loi visant à réduire l'empreinte environnementale du numérique en France (proposition de loi "REEN") définitivement adoptée par le Parlement le 2 novembre et publiée au *Journal officiel* le 16 novembre 2021.

Ce texte qui complète la loi "climat" affiche plusieurs objectifs :
- faire prendre conscience de l'impact environnemental du numérique aux utilisateurs ;
- limiter le renouvellement des terminaux ;
- faire émerger et développer des usages du numérique écologiquement vertueux ;
- promouvoir des centres de données et des réseaux moins énergivores ;
- promouvoir une stratégie numérique responsable dans les territoires.

En matière d'enseignement, la loi impose, d'une part, que la formation à l'utilisation des outils et des ressources numériques dispensée dans les établissements scolaires ou dans le cadre des études supérieures comporte une sensibilisation à l'impact environnemental du numérique ainsi qu'un volet relatif à la sobriété numérique et, d'autre part, que la formation des ingénieurs informatiques comporte un volet relatif à l'écoconception logicielle.

La loi "REEN" prévoit la création d'un observatoire de recherche des impacts environnementaux du numérique qui aura pour mission le recensement et l'analyse des impacts directs et indirects du numérique sur l'environnement ainsi que la contribution apportée par le numérique, notamment l'intelligence artificielle, à la transition écologique et solidaire. Placé auprès de l'Agence de l'environnement et de la maîtrise de l'énergie (Ademe), l'observatoire sera chargé de l'élaboration d'une définition de la sobriété numérique. Ces travaux seront rendus publics et pourront comporter des propositions visant à réduire les impacts environnementaux du numérique.

Pour limiter le renouvellement des terminaux, principaux responsables de l'empreinte carbone du numérique, le texte prévoit le renforcement de la lutte contre l'obsolescence programmée et étoffe sa définition en y intégrant l'obsolescence logicielle. Le recours à des techniques par lesquelles le responsable de la mise sur le marché d'un produit vise à en réduire délibérément la durée de vie pour en augmenter le taux de remplacement était déjà interdit depuis 2016. La loi étend cette interdiction aux logiciels. De plus, plusieurs dispositions de la loi interdisent ou limitent les techniques y compris logicielles dont l'objet serait de restreindre la liberté du consommateur d'installer les logiciels, les systèmes d'exploitation de son choix sur son terminal ou encore les mises à jour de logiciel.

Le texte tend à orienter le comportement des consommateurs et des professionnels du numérique mais aussi celui des acteurs publics. A cette fin, la loi "REEN" prévoit qu'à compter du 1er janvier 2023, lors de l'achat public de certains produits numériques, les services de l'État ainsi que les collectivités territoriales et leurs groupements devront favoriser les biens dont l'indice de réparabilité est supérieur à un certain seuil défini par les dispositions du code de l'environnement.

Et, à compter du 1er janvier 2026, l'indice de durabilité devrait également être pris en compte dans les mêmes conditions.

En outre, la loi du 15 novembre 2021 précise que les équipements informatiques fonctionnels dont les services de l'Etat ou les collectivités territoriales et leurs groupements se séparent devront désormais être orientés vers le réemploi ou la réutilisation. Les équipements informatiques de plus de dix ans seront, quant à eux, destinés au recyclage.

La loi pose également des mesures moins contraignantes relevant plus de l'incitation. Elle prévoit notamment que tout professionnel qui propose à la vente ou à la location des équipements terminaux mobiles neufs doit informer le consommateur de l'existence d'offres d'équipements terminaux mobiles reconditionnés.

Afin de faire émerger et promouvoir les usages numériques écologiquement vertueux, le texte confie à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), au Conseil supérieur de l'audiovisuel (CSA) et à l'Ademe le soin de définir un référentiel général de l'écoconception des services numériques. En s'appuyant notamment sur la définition de l'écoconception prévue à l'article 2 de la directive 2009/125/CE du Parlement européen et du Conseil du 21 octobre 2009(5), le référentiel fixera les critères de conception durable des services numériques afin d'en réduire l'empreinte environnementale. Selon le rapport de la mission d'information, les centres de stockage des données numériques représentaient, en 2019, 14 % de l'empreinte carbone du numérique en France. Le texte propose donc qu'ils s'engagent dans une dynamique de réduction de leurs impacts environnementaux notamment en valorisant la chaleur fatale – chaleur de récupération comme celle des fours et séchoirs –, la chaleur produite et perdue par le site et en limitant la consommation de l'eau utilisée à des fins de refroidissement. De plus, les opérateurs de communications électroniques devront publier les indicateurs clefs de leurs politiques de réduction de leur empreinte environnementale, notamment en matière de réduction des émissions de gaz à effet de serre, de renouvellement et de collecte des terminaux mobiles portables, d'écoconception des produits et des services numériques qu'ils proposent, de recyclage et de réemploi des boîtiers de connexion internet et des décodeurs ainsi que de sensibilisation aux usages responsables du numérique. Enfin, afin de promouvoir une stratégie numérique responsable, la loi du 15 novembre 2021 prévoit l'obligation, à compter du 1er janvier 2025, pour les communes de plus de 50 000 habitants, de définir des objectifs de réduction de l'empreinte environnementale du numérique et les mesures à mettre en place pour y parvenir.

En amont, elles devront, dès le 1er janvier 2023, élaborer un programme de travail préalable à l'élaboration leur stratégie comportant notamment un état des lieux des acteurs concernés et rappelant, le cas échéant, les mesures menées pour réduire l'empreinte environnementale du numérique.

La stratégie numérique responsable fera ensuite l'objet d'un bilan annuel dans le cadre du rapport sur la situation en matière de développement durable présenté avant les débats sur le projet de budget communal.

La loi "REEN" doit cependant être complétée par des dispositions réglementaires, notamment pour les proportions et le calendrier de réemploi des équipements informatiques des administrations ou encore les modalités d'élaboration de la stratégie numérique responsable des communes.

Avant la fin du mois de mai 2022, le Gouvernement remettra au Parlement un rapport sur les mesures qui pourraient être envisagées afin d'améliorer le recyclage, le réemploi et la réutilisation des équipements numériques et sur la faisabilité de ces mesures.

DOCUMENT 15

Incendie et perte de données, les clients d'OVH confrontés aux limites contractuelles
usinenouvelle.com - 23 mars 2021

Après l'incendie survenu dans la nuit du 9 mars, les clients d'OVH touchés pourront-ils obtenir une indemnisation pour les pertes subies ? Ils risquent de se heurter aux limites posées par OVH au sein de ses contrats. Décryptage avec un avocat spécialisé en droit des nouvelles technologies.

La responsabilité d'OVH, premier hébergeur européen, en question

Suite à l'incendie survenu dans le bâtiment principal du datacenter d'OVH situé à Strasbourg (Bas-Rhin) dans la nuit du 9 au 10 mars 2021, des milliers de clients ont perdu, temporairement ou définitivement, leurs données. Les conséquences sont pour certains désastreuses. Pour l'instant, l'heure est au sauvetage technique et OVH temporise avec des gestes commerciaux. La question des recours juridiques des clients touchés se posera sans doute dans un second temps. L'occasion de faire le point sur la responsabilité encourue par OVH.

Une responsabilité définie contractuellement

La responsabilité d'OVH en tant que prestataire technique vis-à-vis de ses clients est de nature contractuelle et n'est pas définie précisément par la loi. Les contours de la responsabilité d'OVH vont donc varier d'un contrat à l'autre, en fonction des options choisies par le client. Selon Me Eric Barbry, avocat en droit des nouvelles technologies et associé du cabinet Racine, *"c'est en fonction du contrat signé que les clients vont savoir quelle est l'ampleur du désastre. Très schématiquement, il y a deux grands types de contrat chez les hébergeurs : soit un contrat d'hébergement simple, sans service associé, soit un contrat d'hébergement avec des services ajoutés (sauvegarde, plan de continuité ou de reprise d'activité – PCA/PRA, Disaster Recovery Plan - DRP, etc…)."*

Les difficultés vont se poser pour les clients ayant conclu un contrat d'hébergement simple, sans service de sauvegarde associé, et qui sont le plus touchés. La question est de savoir si leur contrat d'hébergement simple implique une obligation *a minima* de sauvegarde de leurs données à la charge d'OVH, ou si elle est exclue du champ contractuel. Dans ce dernier cas, ils ne pourront être indemnisés au titre de la perte de données.

Pour Me Eric Barbry, la question de l'étendue de l'obligation d'OVH au titre de l'offre de base doit se poser : *"est-ce que naturellement un contrat d'hébergement doit comporter une prestation de sauvegarde ? Quand un client n'a pas opté pour l'option supplémentaire de sauvegarde, est-ce qu'il est de la responsabilité de l'hébergeur de sauvegarder les données quoi qu'il en soit ? Aujourd'hui, personne ne peut répondre à cette question. OVH dit que ça n'est pas dans sa mission. En cas de recours, ce sera aux tribunaux de déterminer si l'hébergeur doit obligatoirement faire la sauvegarde des environnements qu'il héberge*."

Modification de la politique d'OVHcloud en matière de sauvegarde des données

Le 16 mars, le fondateur et CEO d'OVH a reconnu, dans une vidéo postée sur son compte Twitter, que beaucoup de clients n'avaient pas compris l'offre d'OVH en matière d'hébergement et la nécessité de souscrire à une offre complémentaire de sauvegarde. Octave Klaba a alors annoncé une modification de la politique d'OVH en la matière, afin d'accroître la sécurité des données en offrant le plus haut niveau de sauvegarde de données à tous les clients, sans aucun surcoût. Cette annonce, destinée à rassurer la clientèle pour l'avenir, ne réglera cependant pas la problématique pour les clients qui n'avaient pas souscrit à l'offre de sauvegarde supplémentaire avant la survenance de l'incendie.

La sauvegarde des données sur un même datacenter, une faute contractuelle ?

Pour les clients qui avaient souscrit des options supplémentaires leur assurant la sauvegarde et la récupération des données, les dommages devraient être plus limités. Cependant, il semblerait qu'OVH ait sauvegardé certaines données dans le même datacenter que celui qui hébergeait initialement les données. Certains clients ayant souscrit l'option de sauvegarde auraient donc malgré tout perdu leurs données, du fait de cette localisation. Dans ce cas précis, selon Me Eric Barbry, *"si cela est avéré, la faute contractuelle sera certainement constituée"*.

Plafonds de garantie et force majeure, les limites à la responsabilité d'OVH

Pour empêcher que sa responsabilité soit engagée, OVH pourrait tenter d'opposer aux clients l'exception de la force majeure, l'incendie constituant un accident industriel. Cependant, comme le souligne Me Eric Barbry, *"le feu dans un datacenter, ça n'est pas imprévisible au regard de la nature même de ce type d'installation. Ici, le système de sécurité était manifestement mal dimensionné. A titre personnel, je pense que la force majeure ne pourrait pas être admise."*

Même si les clients parviennent à faire engager la responsabilité contractuelle d'OVH et à écarter la force majeure, les indemnisations seront toutefois limitées par les plafonds de garantie prévus aux contrats, qui seront bien souvent totalement en deçà de la réalité du préjudice économique subi par le client. Dans ce cas, selon Me Eric Barbry, *"le seul moyen pour le client de voir son préjudice pleinement indemnisé sera de tenter de démontrer la faute lourde d'OVH, seule de nature à empêcher l'application du plafond contractuel d'indemnisation*."

Le rôle incertain de la Cnil

Pour Me Eric Barbry, *"la perte de données à caractère personnel est constitutive d'une « violation de sécurité » au sens du RGPD. Les éditeurs de sites web dont les données hébergées ont été détruites devront déclarer cette perte auprès de la Cnil, c'est une obligation. Ce sont les éditeurs de site, en première ligne vis-à-vis de leurs clients, qui supporteront la responsabilité de la perte de données. La question va toutefois se poser de savoir si les responsables de traitements vont pouvoir reporter cette responsabilité sur OVH en tant que prestataire technique sous-traitant*."

Pour l'heure, il est cependant difficile de savoir à quel point la Cnil va s'impliquer au vu de ces déclarations de violations de sécurité, et si elle ira jusqu'à prononcer des sanctions, en l'absence vraisemblable de tout élément intentionnel dans cet incident.