Cloud et administrations publiques : entre souveraineté et externalisation

Nicolas Savoy, le 11 janvier 2021

Les solutions informatiques dans le nuage sont désormais légion. Depuis une dizaine d'année, le cloud s'est imposé, notamment par l'entremise des grands acteurs IT que sont Google, Amazon, Oracle ou encore Cisco. Il n'en va pas différemment pour Microsoft : avec la suite Office 365 et Windows 10, la firme de Redmond a elle aussi fait le pari du cloud. Si l'utilisation du cloud est devenue monnaie courante dans le monde des entreprises privées, qu'en est-il des administrations publiques ? Le choix de cette technologie est loin d'être anodin.

Introduction

Les administrations publiques, à l'instar du secteur privé, n'échappent pas à la modernisation de leurs infrastructures et de leurs processus. À l'interne, les solutions informatiques utilisées doivent évoluer, pour des raisons de sécurité, de support, de coûts, d'efficacité et d'expérience utilisateur. S'agissant de l'État de Vaud, le Plan directeur cantonal des systèmes d'information et la Stratégie numérique de la Direction Générale du Numérique et des Systèmes d'Information (DGNSI) guident et orientent les actions à effectuer en tenant compte d'une multitude de principes, comme la sécurité, la protection des données ou encore la gouvernance du numérique.

Les solutions informatiques dans le *cloud* permettent une rationalisation et une prévisibilité des coûts ainsi qu'une souplesse au niveau du déploiement, des mises à jour, de l'adaptation et du maintien de la solution considérée. En effet, la création et l'hébergement de solutions informatiques à l'interne d'une organisation n'est pas toujours possible ni pertinent d'un point de vue technique ou économique.

De manière plus générale, que cela soit sous la forme de *SaaS*, *IaaS*, *PaaS* ou *DaaS*, de plus en plus de solutions informatiques sont désormais proposées dans le *cloud*. Pour les administrations publiques, le choix de cette technologie exige une réflexion large, que ce soit au niveau de la protection des données, du secret de fonction, de l'aspect contractuel, de l'application de règles sur les marchés publics ou encore pour des raisons d'opportunité politique et technique.

Protection des données

1. Généralités

L'emploi d'un service basé dans le *cloud* proposé par un fournisseur externe à l'administration est une forme de sous-traitance. Le sous-traitant est défini comme une « *personne physique ou morale, autorité publique ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement* » conformément à l'art. 4 al. 2 ch. 9 de la loi vaudoise du 11 septembre 2007 sur la protection des données (LPrD), s'agissant d'un traitement de données personnelles effectué par une entité publique vaudoise. Le service « métier » de l'administration qui en fera usage sera le responsable de traitement au sens de l'art. 4 al. 2 ch. 8 LPrD.

Conformément à l'art. 18 LPrD, un traitement de données personnelles peut être confié à un tiers si le traitement est prévu par la loi ou un contrat, si le responsable de traitement est lui-même légitimé à traiter les données concernées et qu'aucune obligation légale ou contractuelle ne l'interdit. Cette disposition trouve pleinement application dans le cadre d'une utilisation d'un service dans le *cloud* par une administration publique.

Le service « métier » de l'administration qui désire opter pour une solution externalisée dans le *cloud* cherche bien souvent à moderniser une activité ou une tâche publique qu'il effectuait déjà. Il est donc légitimé à envisager de basculer cette activité dans le *cloud*. Au stade préliminaire, une étude des solutions locales et étrangères existantes doit être menée, en effectuant une pesée d'intérêts qui tient compte des éléments suivants, en sus de la nécessaire protection des données :

- opportunité de faire appel à un prestataire externe ;
- intégration avec les systèmes d'information existants ;
- mesures techniques et organisationnelles de sécurité ;
- migration des données ;
- disponibilité de la solution externalisée ;
- application des règles sur les marchés publics ;
- dispositions sectorielles propres au service métier bénéficiaire.

Dans la plupart des cas, il existe un contrat avec le fournisseur de la solution qui règle principalement les aspects commerciaux et techniques. En sus, le fournisseur peut parfois proposer un contrat de sous-traitance des données personnelles annexé au cadre contractuel, sous la forme d'un « *Data Processing Agreement* » ou « *Data Protection Addendum* ».

S'il existe, une vérification des dispositions s'impose, notamment sur les éléments suivants : détermination des parties, finalité du traitement, obligations des parties, éventuelle sous-traitance ultérieure, lieu de traitement et d'hébergement des données, droit de contrôle d'une autorité de surveillance, droits des personnes concernées, responsabilité, fin du contrat ou encore for et droit applicable.

S'il est incomplet, insatisfaisant ou inexistant, des amendements respectivement une proposition de contrat doivent être amenés.

2. Problématiques choisies

a) Le recours à une solution externalisée dans le *cloud* implique une perte de maîtrise au moins partielle sur les données personnelles sous-traitées. Dès lors, le choix du fournisseur et le lieu d'hébergement deviennent des questions critiques tant d'un point de vue juridique que politique. Or, beaucoup de fournisseurs sont étrangers. Un hébergement et un traitement sur le territoire suisse, pour des raisons de souveraineté et de secret de fonction, est souhaitable. Nous insistons également sur la nécessité de prévoir un for en Suisse et l'application du droit suisse.

b) Si le fournisseur propose une option de chiffrement des données personnelles, le principe de précaution implique de considérer que le fournisseur aura de toute manière accès aux données personnelles, malgré la présence de garanties contractuelles. En effet, ces dernières ne seront d'aucun secours en cas de requête judiciaire au lieu d'hébergement, surtout à l'étranger. Ce point est particulièrement critique en matière de données ou d'informations soumises au secret de fonction. Le chiffrement effectué par l'administration dont elle seule possède la clé serait un moyen de parer à toute éventualité de ce type. Cependant, peu de fournisseurs proposent cette possibilité, qui est par ailleurs complexe à gérer pour l'administration. Pour une analyse détaillée sur la question du secret de fonction dans ce cadre, nous renvoyons à la contribution du Prof. Sylvain Métille sur le sujet.

c) La sous-traitance en cascade, ou sous-traitance ultérieure, peut être problématique dans le cadre de communications transfrontières de données personnelles. En effet, si le sous-traitant « primaire » héberge les données en Suisse ou du moins dans un pays considéré comme adéquat, il peut faire appel à ses propres sous-traitants pour effectuer un service de support « *follow-the-sun* » ou « 24/7 ». Or, de ce point de vue, il est tout-à-fait concevable que des opérateurs du sous-traitant ultérieur puissent avoir accès aux données personnelles depuis des pays qui ne sont pas considérés comme offrant un niveau de protection des données adéquat. En outre, il s'agit d'identifier soigneusement ces éventuels sous-traitants ultérieurs

et s'assurer qu'ils sont bel et bien soumis aux mêmes exigences en matière de protection des données que le fournisseur primaire. Il convient de préciser que l'art. 9 al 3 nLPD prévoit l'interdiction de principe de la sous-traitance en cascade. Il n'est pas à exclure que la LPrD, actuellement en révision elle aussi, prévoie le même régime en la matière.

d) Si le fournisseur est étasunien, nous rappelons que le Privacy Shield a été annulé par la CJUE en juillet 2020, dans l'affaire C-311/18 « Schrems II ». Si cette décision n'a pas d'effet direct en Suisse, le Préposé fédéral à la protection des données et à la transparence estime que le Privacy Shield US – CH, dès l'instant où il s'agit de l'équivalent européen, n'est plus un mécanisme adéquat pour un transfert de données vers les États-Unis. Dès lors, en cas de recours à des *Standard Contracual Clauses* (SCC) pour encadrer le transfert, une analyse de risques est obligatoire. Pour plus de détails, nous renvoyons aux excellentes contributions de Philipp Fischer et Philipp Fischer / Kastriot Lubishtani.

e) La fin du contrat doit être soigneusement étudiée. En effet, les données (personnelles ou non) sont hébergées sur des systèmes externes. Dans ce cas, il s'agit de prévoir tous les processus qui permettront de rapatrier les données de manière optimale. Cela procurera à l'administration le temps et les ressources nécessaires pour choisir un autre prestataire ou de créer sa propre solution. En outre, et cela peut sembler à première vue trivial, il s'agira d'exiger du fournisseur que les données soient rapatriées dans un format qui permet de les utiliser dans le nouveau système. La collaboration étroite et proactive du prestataire est dans ce cas fondamentale.

Conclusion

Le choix de la technologie *cloud* est une décision importante qui mérite une réflexion pluridisciplinaire. Si le service en charge du numérique et des systèmes d'information de l'entité publique sera en première ligne pour l'évaluation et le choix, il nous semble important d'impliquer le plus tôt possible le service « métier » qui utilisera la solution. Une étude soigneuse des différents aspects juridiques (protection des données, contrats, marchés publics et secret de fonction) et d'opportunité technique, économique et politique doit être menée.

Enfin, le *cloud* dans le contexte des administrations publiques est un sujet central dans les réflexions numériques actuelles au niveau national : au printemps 2020, le Conseil fédéral, bien conscient des problématiques liées à cette technologie, a chargé le Département fédéral des finances (DFF) d'examiner en détail la nécessité et la faisabilité d'un *Swiss Cloud*. Il est ressorti de cette étude la pertinence de la création d'un label « *Swiss Cloud* » et

l'identification des critères auxquels un prestataire labélisé devrait satisfaire, notamment : fournisseur majoritairement en mains suisses et qui ne doit pas être soumis à des obligations de communications des données à des tiers, le tout avec un for et un droit suisse applicable.

Proposition de citation : Nicolas Savoy, Cloud et administrations publiques : entre souveraineté et externalisation, 11 janvier 2021 *in* www.swissprivacy.law/48