AWK Group
Enabling digital performance.

Cloud Souverain

Étude d'opportunités pour un cloud souverain

Sur mandat de la Conférence latine des directrices et directeurs cantonaux du numérique

Date de publication : 11.05.2023

Informations sur le document

Titre :	Étude d'opportunités pour un cloud souverain
Date de publication :	Date de publication : 11.05.2023
Sauvegardé :	11. mai 2023
Nombre de pages :	51, sans les annexes
Nom du fichier :	Étude d'opportunités pour un cloud souverain
Représentants du mandant :	Catherine Pugin, Déléguée au numérique pour le Canton de Vaud Alexander Barclay, Délégué au numérique pour le Canton de Genève
Auteurs :	Nicolas Savoy, Juriste protection des données, DGNSI (chapitre 3) Anthony Buchard, Consultant Digital Strategy & Innovation, AWK Group Fabian Heiniger, Managing Consultant, AWK Group Jesko Mueller, Managing Consultant, AWK Group Blaise Vonlanthen, Head of Romandie, AWK Group

Versions

Version	Date	Changements importants	Responsable
V0.0	07.03.2022	Initialisation et structure du document	Équipe d'auteurs AWK
V0.1	23.05.2022	Élaboration initiale du contenu de l'étude sur la base des analyses et des entretiens effectués	Équipe d'auteurs AWK
V0.2	02.06.2022	Consolidation de tous les résultats des entretiens et des analyses	Équipe d'auteurs AWK
V0.3	17.06.2022	Élaboration des opportunités	Équipe d'auteurs AWK
V0.4	27.06.2022	Intégration du chapitre cadre juridique dans l'étude	Nicolas Savoy, Équipe d'auteurs AWK
V0.5	04.07.2022	Consolidation des retours par la revue interne AWK	Équipe d'auteurs AWK
V0.6	09.08.2022	Consolidation des retours par l'équipe de projet	Équipe d'auteurs AWK
V0.9	26.08.2022	Finalisation de la version 0.9	Équipe d'auteurs AWK
V0.95	27.09.2022	Consolidation des retours par l'équipe de projet	Équipe d'auteurs AWK
V0.96	04.01.2022	Consolidation de retour	Équipe d'auteurs AWK
V1.0	16.01.2022	Finalisation	Équipe d'auteurs AWK

AWK GROUP AG
Avenue de la Gare 33, CH-1003 Lausanne,
T +41 58 411 95 00, www.awk.ch
Zurich • Bern • Basel • Lausanne

Documents de référence

Titre	Auteur / Editeur	Date	Lien
[1] Rapport sur l'évaluation des besoins d'un nuage informatique suisse (« Swiss Cloud »)	Chancellerie fédérale	11.03.2021	Lien
[2] Étude académique sur la souveraineté numérique	Uni GE	En cours d'élaboration	
[3] Étude de marché et variantes	AWK Group AG	08.2022	
[4] BMWi-Schwerpunktstudie 2021 Digitale Souveränität	Bundesministerium für Wirtschaft und Energie (BMWi)	09.2021	Lien
[5] Prestataires de services d'informatique en nuage (SecNumCloud)	Agence nationale de la sécurité des systèmes d'information (République Française)	08.03.2022	Lien
[6] European Secure Cloud – a new label for cloud service providers	Agence nationale de la sécurité des systèmes d'information (République Française) et Bundesamt für Sicherheit in der Informationstechnik (Deutschland)	08.2022	Lien
[7] Documentation des entretiens menés dans le cadre de l'étude	AWK Group AG	08.2022	

Sommaire

1. Management Summary

Le débat sur les risques liés aux données des administrations dans le *cloud* est un sujet d'actualité en Suisse et en Europe. Les recours croissant à des fournisseurs de solutions informatiques, la concentration du marché sur quelques grands fournisseurs mondiaux (les *hyperscalers*) ainsi que les nouvelles compétences qui sont nécessaires à la gestion de ces solutions nourrissent des inquiétudes quant à la souveraineté des administrations publiques. La pratique montre qu'il est difficile pour une administration publique de se détourner complètement des technologies et des solutions en nuage informatique (ci-après technologies et solutions cloud), car elles sont porteuses de valeur ajoutée pour les métiers, en augmentent leur efficacité et permettent d'innover dans de nombreux domaines d'activité. Toutefois, il convient de considérer les enjeux amenés par une transition vers le *cloud* (voir chapitre 0). La tendance montre que les solutions *on-premise*[1] utilisées aujourd'hui seront à l'avenir de plus en plus proposées uniquement dans le *cloud*. Les administrations publiques sont donc contraintes d'agir et de faire le pas vers le *cloud* si elles souhaitent pouvoir continuer de bénéficier de certaines solutions ou de trouver des solutions alternatives. Elles ne peuvent pas maintenir le statu quo si elles veulent continuer à évoluer et répondre aux fortes attentes des citoyen-ne-s, des entreprises et du personnel des administrations.

Comment alors garantir la souveraineté d'une administration cantonale – ou publique au sens large – dans le contexte de solutions cloud ? Cette étude se penche sur cette question avec l'objectif initial d'analyser les opportunités pour la mise en œuvre d'un *cloud* « souverain ». D'après les entretiens menés avec des représentants informatiques d'administrations[2] publiques, d'institutions[3] parapubliques, ainsi qu'avec des fournisseurs locaux et globaux de solutions informatiques et *cloud*, il a été constaté qu'il n'y a pas de consensus sur les éléments de base de cette question : il ne règne pas de compréhension commune lorsqu'il s'agit de la signification de la souveraineté numérique, ni des services et cas d'usage qu'un *cloud* « souverain » devrait fournir. C'est pourquoi, les auteurs de cette étude se sont focalisés d'une part à formaliser la notion de souveraineté numérique et d'autre part à élaborer un modèle[4] visant à soutenir les administrations publiques et parapubliques dans la définition de leurs exigences respectives envers la souveraineté numérique. Celle-ci peut être appliquée à des systèmes d'information et cas d'usage qu'ils soient *cloud* ou non.

Dans le cadre de la présente étude, la souveraineté numérique est définie comme suit :

> La souveraineté numérique est la capacité d'autodétermination d'une entité (légale) en ce qui concerne tout le cycle de vie d'un système numérique, de la conception à l'utilisation au décommissionnement de systèmes numériques et des données qui sont traitées et stockées ainsi que des processus qu'ils représentent.

Cette définition, s'inscrivant dans une étude d'intention technique, pourrait être élargie ultérieurement pour poser la souveraineté numérique dans un cadre plus large.

De cette définition découlent douze dimensions de la souveraineté numérique, qui permettent de définir les exigences en matière de souveraineté numérique : Développement du système, Durabilité, Traitement des données, Localisation des données, Disponibilité du système, Accès au système et aux données, Gestion de l'évolution, Stratégie exit, Extraction des données, Cadre juridique, Expertise et Contrats.

L'application de la définition de la souveraineté numérique à une solution cloud n'apporte pas de réponse unique et il n'existe donc pas non plus de solution unique à la question initiale de l'étude

---

[1] Le terme « on-premise » signifie littéralement « dans les locaux ». Dans ce modèle d'utilisation, l'utilisateur achète ou loue un logiciel qui sera installé sur son propre serveur.

[2] Cantons de Vaud, Genève, Valais, Fribourg, Neuchâtel, Jura et Ville de Genève

[3] Hôpitaux universitaires de Genève

[4] Le modèle de la souveraineté numérique développé dans cette étude se compose d'une démarche (chapitre 5.5) pour définir les exigences en matière de souveraineté numérique et d'un cadre d'analyse (chapitre 4.3).

(opportunités pour « un *cloud* souverain »). Cela est dû au fait qu'il n'existe pas de niveau de souveraineté unique applicable à tous les cas d'utilisation. Ainsi, une administration publique doit, pour chaque cas d'utilisation, analyser le niveau d'exigence de souveraineté qui lui est nécessaire. Il est possible pour une administration publique d'examiner comment mettre en œuvre une solution cloud souveraine dès lors que le degré de souveraineté exigé est défini.

Cette étude fournit donc aux administrations cantonales des variantes de mise en œuvre qui couvrent différents niveaux de souveraineté. Quatre types de variantes sont caractérisés, qui correspondent à l'offre actuelle du marché local et global[5], des possibilités de mise en œuvre en interne et qui sont réalisables pour les administrations publiques.

Finalement, l'étude émet des recommandations en vue de faire avancer la thématique de la souveraineté numérique dans le secteur public. Ainsi, la présente étude recommande les champs d'actions suivants :

- Élaborer des principes et stratégies cantonales pour l'utilisation de services *cloud* pour les administrations
- Identifier les cas d'usage pour l'utilisation de services *cloud* et effectuer une classification détaillée des données
- Identifier les synergies et les opportunités pour l'utilisation de services *cloud* pour toutes les administrations cantonales par un broker
- Créer un référentiel

[5] Une étude de marché a été réalisée dans le cadre de cette étude. Les résultats sont disponibles dans [3].

2. Introduction

2.1. Situation initiale

L'importance stratégique des technologies numériques pour les organisations publiques et parapubliques ainsi qu'une série d'évènements récents font aujourd'hui de la notion de « souveraineté numérique » un objet d'un fort intérêt dans les milieux politiques, scientifiques et économiques en Europe. En Suisse, les cantons latins, par le biais de la Conférence latine des directeurs du numérique (CLDN[6]), souhaitent aujourd'hui adresser et approfondir les enjeux, les opportunités et les risques des technologies cloud, sous l'angle de la souveraineté numérique.

Le dossier « Swiss Cloud[7] » fut le principal déclencheur de la discussion entamée au sein de la CLDN. Ce dossier, qui fut mené par la Chancellerie fédérale, avait pour objectif d'évaluer les besoins, la conception, la nécessité et la faisabilité d'une solution étatique d'informatique en *cloud*. Des experts de l'économie, de la recherche et des administrations publiques des trois niveaux de l'État y avaient participé. La Confédération a évalué que la nécessité d'un « Swiss Cloud » sous forme d'une infrastructure technique indépendante de droit public et comme facteur de succès pour la place économique suisse n'est pas démontrée. Un examen supplémentaire a été mené pour déterminer s'il était nécessaire de créer un système de certification pour les services en nuage. Selon la Confédération, cet examen n'a pas mis en évidence un besoin concret de réglementation étatique. En parallèle, avec le projet « Public Clouds Confédération » l'Administration fédérale a fait le choix acquérir de manière flexible des services informatiques cloud très évolutifs pendant cinq ans. Les entreprises Microsoft, Oracle, IBM, Amazon et Alibaba ont remporté le marché pour un cloud public avec un volume de 110 millions de francs. Aucune entreprise suisse n'a participé à l'appel d'offres[8]. Toutefois, ce dossier fait actuellement l'objet d'une procédure au Tribunal fédéral, notamment sur la question de la base légale. Le Tribunal fédéral a renvoyé le dossier au Tribunal administratif fédéral, qui devra se pencher sur le contenu du recours[9].

Les discussions autour de la souveraineté en matière de *cloud* ne sont aujourd'hui pas terminées, mais bien au contraire étant donné le contexte géopolitique dans lequel se trouve actuellement l'Europe. Les questions et les enjeux liés à l'utilisation des technologies cloud pour les administrations publiques et parapubliques suscitent le débat tant au niveau politique qu'au sein des administrations. En effet, les organisations informatiques de ces dernières font face à d'importants défis. D'une part, les produits de certains éditeurs de logiciels et de services informatiques sont de plus en plus proposés sous forme de technologies cloud alors que, d'autre part, les directives et réglementations cantonales et fédérales actuelles ne permettent pas toujours une transition vers le *cloud* en toute légitimité et conformité. Aujourd'hui, une ligne directrice et un cadre clair pourraient permettre aux organisations informatiques des administrations publiques et parapubliques de s'orienter.

Les Cantons latins souhaitent donc mener une réflexion globale sur la souveraineté numérique liée aux technologies cloud, sur la base de cas d'usage concrets, afin d'apporter de la clarté sur les enjeux, les opportunités et les risques. En ce sens, il s'agit de mener une démarche qui tient compte des aspects juridiques, politiques, économiques et technologiques afin de nourrir le débat. Il convient de noter qu'une étude académique est réalisée en parallèle afin d'adresser les aspects juridiques et socio-économiques ([2]).

Il s'agit de décliner une définition de la souveraineté numérique, de sorte à ce que chaque administration publique ou parapublique puisse déterminer son niveau de souveraineté numérique par

[6] https://cldn.ch/

[7] https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

[8] https://www.ictjournal.ch/news/2021-10-21/cloud-de-la-confederation-le-recours-de-google-naura-pas-deffet-suspensif

[9] https://www.ictjournal.ch/news/2022-08-16/le-tribunal-administratif-federal-devra-statuer-sur-le-projet-de-cloud-public-de-la

rapport à son contexte, à sa vision et à sa sensibilité et interprétation de la notion de souveraineté numérique.

2.2. Objectifs de l'étude

La présente étude a pour objectif d'explorer la thématique d'un cloud souverain et de susciter la compréhension commune des membres de la CLDN. Cette compréhension commune est une base nécessaire pour ensuite pouvoir évaluer les enjeux et les opportunités qui en découlent. En d'autres termes, la présente étude doit d'une part permettre de nourrir le débat politique en amenant une compréhension commune des enjeux et opportunités et permettre la mutualisation de stratégies et solutions. D'autre part, elle doit permettre aux administrations publiques et institutions parapubliques de déterminer quelles sont les variantes de mise en œuvre possibles afin de garantir leur niveau de souveraineté numérique adéquat et adapté à chaque cas d'usage spécifique.

Dans cette perspective, les institutions publiques et parapubliques intéressées par la souveraineté numérique liée aux technologies cloud pourront y trouver les argumentations et réflexions nécessaires concernant l'utilisation souveraine des technologies cloud. Par ailleurs, le présent document permettra également aux lecteurs de disposer d'un outil pour déterminer leur niveau de souveraineté souhaité en fonction de leur contexte et d'en comprendre les opportunités et les risques liés.

Finalement, cette étude présente également une brève étude de marché (voir [3]) sur les principaux fournisseurs de service cloud en suisse et notamment en Suisse romande. L'étude de marché met en perspective l'offre de services des fournisseurs suisses avec celles des *hyperscaler* afin d'en relever les différences.

2.2.1. Public cible

La présente étude est destinée aux publics cibles ci-dessous :

- Les responsables politiques y trouveront des informations pour approfondir le thème du cloud souverain ainsi que ses tenants et aboutissants afin de pouvoir prendre position sur les questions nécessaires pour aller de l'avant.
- Les organisations informatiques des cantons et des institutions parapubliques y trouveront des informations pour rendre l'utilisation des technologies cloud plus souveraine ou pour alimenter le dialogue politique de leur canton.
- Le grand public intéressé par la notion de souveraineté numérique liée aux technologies cloud y trouvera des informations sur les différents enjeux concernant le cloud souverain.

2.2.2. Méthodologie

La présente étude se base sur les éléments recueillis des entretiens avec des interlocuteurs du secteur public et parapublic, avec des fournisseurs de services cloud et avec des experts sur le thème de la souveraineté numérique et du cloud. La liste des interlocuteurs se trouve en annexe A.1. En outre, les rapports et les analyses mentionnés dans les documents de références ont été consultés afin d'éclairer le sujet de la souveraineté selon différents angles et ainsi enrichir l'argumentation avec des faits établis dans la pratique et la recherche.

2.2.3. Délimitation

Les aspects éthiques, politiques et économiques de la souveraineté numérique sont adressés par une démarche académique menée par les Professeur Yaniv Benhamou, Professeur Frédéric Bernard et Professeur associé Cédric Durand (Université de Genève) et son équipe. Certains aspects légaux pertinents pour la discussion de la souveraineté numérique sont présentés dans le chapitre 3.3. Toutefois, ce chapitre n'en présente pas une analyse détaillée complète.

2.2.4. Hypothèse et questions de recherche

La présente étude est basée sur les deux hypothèses suivantes :

- Un *cloud* répondant à la notion de souveraineté numérique est nécessaire pour les administrations cantonales et les institutions parapubliques.
- La souveraineté numérique est considérée dans la perspective d'un contexte géopolitique stable (voir 4.2).

La présente étude vise à répondre aux questions de recherche suivantes, qui regroupent une large liste de questions présentée en annexe 0 :

- Que signifie la souveraineté numérique ?
- Quelle est la définition d'un cloud souverain et qu'est-ce qui le caractérise ?
- Quelles sont les variantes possibles pour garantir la souveraineté de différents cas d'usage *cloud* ?

3. L’utilisation du cloud dans les institutions publiques et parapubliques

Le *cloud computing* se compose d’un ensemble de technologies, d’infrastructures et de compétences qui permettent de mettre à disposition des consommateurs une offre de services numériques sous forme de location. L’utilisation de technologies cloud induit des changements importants au sein des institutions publiques et parapubliques, notamment au niveau de la gestion de la relation client-fournisseur, des modes de financement imposés par les prestataires de services cloud et dans la façon de réaliser et d’exploiter des services numériques. Il s'agit en ce sens d’un changement de paradigme à bien des égards, qui soulève des questions d’ordre juridique, politique et économique – en particulier lorsqu’il s’agit de services cloud de prestataires dont le siège se trouve au-delà de la Suisse ou de l’Europe.

Sur la base des entretiens réalisés avec les interlocuteurs publics et parapublics et de l'analyse de leur stratégie numérique (ou similaires), il a été constaté que la prise en compte au niveau stratégique, les défis identifiés, les ambitions mais aussi les possibilités de développement dans le *cloud* varient fortement d’un canton à l’autre. Les raisons sont diverses et dépendent notamment de leurs moyens financiers et organisationnels, de priorités politiques et de leur cadre réglementaire. La section suivante présente le panorama des perceptions relevées lors des entretiens.

3.1. Perception des cantons latins

Divers acteurs des cantons latins (Jura, Neuchâtel, Vaud, Genève, Fribourg, Valais et Tessin) ont été interviewés pour relever leur perspective en matière d’utilisation et de souveraineté liées aux services cloud au sein de leur administration respective. Les entretiens menés ont permis de relever des approches très différentes parmi les cantons dans la façon d’adresser le thème du cloud. En effet, un canton a mené une démarche lui permettant de créer une base légale pour traiter les données dans le *cloud* en toute conformité. La majorité des autres Cantons interviewés, lorsqu’ils recourent à des services cloud, le font sur la base d’une analyse des opportunités et des risques propres à chaque cas d’usage, sans toutefois disposer d’un cadre juridique ni d’un positionnement politique clairement et définitivement établi.

Les sections suivantes présentent une synthèse des principaux éléments relevés lors des entretiens, regroupés selon les cinq dimensions : *Vision politique*, *Marché des services cloud*, *Besoins de recourir au cloud*, *Besoin d’un cloud souverain* et *Impacts organisationnels*.

Les résultats détaillés des interviews se trouvent dans le document [7].

3.1.1. Vision politique

Les personnes interrogées au sein des administrations cantonales constatent aujourd’hui qu’elles n’ont pas accès à des directives claires et qu’il est de leur responsabilité de fournir l’expertise nécessaire à leurs responsables politiques pour qu’ils puissent prendre des décisions informées. Associées à une vision et une stratégie définies, ces directives sont nécessaires pour une utilisation des services cloud conforme et pertinente, à la mesure des enjeux. Dès lors qu’il n’y a pas de vision et de directive commune, chaque canton gère la thématique du *cloud* à sa façon avec les moyens disponibles et les ambitions qui lui sont propres.

Les échanges et discussions entre l’administration cantonale et leur instance politique sur le thème du *cloud* et du cloud souverain sont dans certains cas très limités, voire inexistants. La difficulté à utiliser des services cloud dans le secteur public n’est pas d’ordre technique mais politique et juridique. En effet, l’utilisation de services cloud de fournisseurs suisses ou étrangers nécessite un positionnement des responsables politiques sur les aspects économiques, sociaux et juridiques, entre autres.

Les entretiens menés dans le cadre de l'étude relèvent un niveau de compréhension et de sensibilité quant aux notions de « cloud » et de « souveraineté », qui diffère d'une institution à l'autre. En effet, pour certaines institutions, la souveraineté numérique s'applique à la question de la protection des données alors que pour d'autres, elle relève de manière plus large de l'application des lois[10]. Les citoyens font preuve de confiance envers leur administration informatique qu'elle agisse souverainement dans le numérique en général mais surtout en termes de protection des données. Chaque administration informatique garantit le respect des lois pour la protection des données, mais celles avec plus de moyens ont la possibilité de considérer des solutions plus complexes à travers le cycle de vie d'un service cloud. La compréhension du *cloud* est inégale au niveau des citoyens et des métiers en raison de la complexité technique, mais différentes initiatives[11] d'intégrité numérique visent à améliorer cette compréhension et à nourrir le débat sur ces thèmes. Ces initiatives sont souvent menées par des responsables politiques avec des intérêts particuliers au numérique.

3.1.2. Marché des services cloud

Les administrations cantonales sont aujourd'hui fortement liées à des produits (p. ex. SAP, Microsoft Office, DeepL.com, etc.) dont les versions actuelles et futures se baseront principalement sur des technologies cloud. Le coût de certaines solutions *on-premise* augmente et leur périmètre fonctionnel n'évolue plus ou n'est plus garanti à moyen/long terme. Cette tendance pose le dilemme suivant aux administrations publiques :

- Continuer de bénéficier des (nouvelles) fonctionnalités des produits et donc accepter le changement technologique qui s'ensuit, c'est-à-dire la transition d'une installation *on-premise* vers une solution cloud.
- Changer pour une solution alternative non-cloud avec les risques et les opportunités qu'un tel changement de grande envergure peut apporter au niveau des coûts, de la qualité, de la sécurité, etc.

3.1.3. Besoins de recourir au cloud

Les services cloud sont un moyen permettant aux organisations IT des administrations cantonales d'étendre leur capacité à répondre à la forte demande de numérisation des métiers. Ce besoin s'observe notamment dans les plus petits cantons où l'effectif en matière de personnel ou de compétences IT spécifiques n'est pas toujours disponible en suffisance pour répondre à la demande en constante augmentation de leurs métiers.

Les collaborateur-trice-s des administrations cantonales souhaitent pouvoir bénéficier de services cloud pour différentes raisons (innovation, rapidité de mise en place, expérience similaire avec utilisation privée, etc.). Afin de répondre au besoin des métiers et pour éviter toute utilisation de services cloud non-maîtrisée, les administrations cantonales et plus particulièrement leur organisation IT se doivent de garantir que l'accès à des services cloud se fait dans un environnement maîtrisé.

Les services cloud permettent de mutualiser des infrastructures et des prestations novatrices entre plusieurs cantons. En effet, certaines institutions (p. ex. ville et services industriels) utilisent des services cloud pour bénéficier d'une plateforme commune afin de valoriser les données qui y sont traitées[12].

---

[10] Les déclarations suivantes ne proviennent pas d'une enquête et d'une analyse à grande échelle, mais sont des déclarations consolidées issues des entretiens réalisés. Voir [7].

[11] Par exemple : Digital Days Switzerland : https://digitaltage.swiss/fr/

[12] Par exemple : Des initiatives de « Smart City » dans différentes grandes villes suisses avec des communes suburbaines, couvrant par exemple le développement de quartiers énergiquement intelligents et le développement de territoires connectés ainsi que la mise à disposition de l'infrastructure pour les différentes parties prenantes

Les personnes interrogées dans le cadre de l'étude s'accordent de manière large sur le fait que l'accès à des services d'intelligence artificielle ou de big data nécessitent et/ou nécessiteront l'utilisation de services cloud.

Certaines administrations cantonales perçoivent le niveau de qualité et de sécurité des services cloud plus élevés que les services développés en interne. En effet, les moyens financiers dédiés par les fournisseurs de services cloud à la sécurité et à l'innovation ne sont pas comparables aux moyens dont disposent les administrations cantonales.

3.1.4. Besoin d'un cloud souverain

Les personnes interrogées considèrent le *cloud* comme un nouvel outil technologique qu'ils considèrent au même titre que d'autres nouveaux outils. La notion de souveraineté dans le *cloud* doit être alignée avec celle de la souveraineté numérique. Les personnes interrogées souhaitent que l'administration cantonale puisse accomplir ses missions à l'aide d'applications métiers du marché qui migrent sur le *cloud*.

Il est communément admis que l'open source est une solution pour garantir la souveraineté, mais les conséquences en termes d'innovation et d'effort de réalisation sans passer par un intégrateur ne sont pas comparables.

Certains cantons entendent, par *cloud* souverain, une infrastructure nationale pour les services de base qui doit être mise à disposition sous forme de solution nationale pour tous les cantons avec un paramétrage spécifique au niveau cantonal, laissant ainsi l'autonomie aux cantons quant aux services métiers. Cette infrastructure nationale serait pilotée sous la gouvernance d'un conseil administratif composé de représentants nationaux et cantonaux ainsi que d'actionnaires. Ainsi, un *cloud* souverain devrait pouvoir offrir des services de base de manière centralisée.

Selon certains cantons, le *cloud* souverain devrait garantir la maîtrise et la protection des données de la population. Ainsi, le niveau de souveraineté d'un service basé sur du *cloud* livré par un fournisseur doit être auditable et labelisé.

3.1.5. Impact organisationnel

Le recours à des services *cloud* impacte les organisations IT des administrations cantonales. En effet, les organisations IT doivent disposer de plus en plus de profils juridiques pour négocier et contractualiser les prestations avec les fournisseurs de services cloud. Certains profils techniques (p. ex. ingénieur messagerie) tendent à être remplacés par des profils de gestionnaires de service qui pilotent la relation avec le fournisseur et les niveaux de service définis. Les effectifs des ingénieurs système augmentent pour répondre au besoin d'intégrer les services cloud dans les systèmes d'information au rythme imposé par les fournisseurs de services cloud.

Les entretiens montrent également que la gestion des données et notamment la classification des données au sein des administrations cantonales sont cruciales pour acquérir les services cloud en toute conformité. Cela nécessite une démarche transverse à l'administration cantonale dans laquelle les métiers et l'organisation IT collaborent pour cartographier les données métiers, en vue d'acquérir les services cloud avec pertinence.

La frontière entre l'organisation IT et les métiers d'une administration cantonale diminue dans la perspective des services cloud, car ceux-ci peuvent parfois être acquis simplement et rapidement, ne nécessitant pas de grandes compétences informatiques. Partant, les administrations cantonales souhaitent disposer d'un cadre et de directives les guidant d'une part dans le choix des services cloud à utiliser selon les cas d'usage et d'autre part à définir la gouvernance pour acquérir et piloter ces services cloud.

3.2. Enjeux

De nombreux enjeux se posent en matière d'utilisation des technologies cloud dans le secteur public. Le panorama ci-dessous doit permettre de présenter la variété des défis, mais aussi des opportunités en matière de *cloud*.

3.2.1. Dépendance envers les prestataires de services cloud

Les possibilités du *cloud* ont fait évoluer les modèles d'affaires des prestataires de services informatiques. Alors qu'auparavant, les institutions publiques et parapubliques étaient propriétaires de leurs solutions en les installant au sein de leur propre infrastructure, elles sont aujourd'hui locataires de services, qui se trouvent généralement dans des infrastructures cloud de prestataires locaux ou globaux. Cette tarification sous la forme d'abonnement lie les institutions publiques et parapubliques plus fortement aux prestataires. Par ailleurs, certains prestataires, qui jusqu'ici offraient des solutions pouvant être installées *on-premise*, déplacent aujourd'hui de plus en plus de services de leur offre dans des infrastructures cloud, ne laissant pas forcément d'alternatives à leurs clients s'ils souhaitent continuer de profiter de ces mêmes services. La substitution par un autre service s'avère souvent bien trop coûteuse financièrement, ou ne présente pas la même qualité de service.

Bien que ce changement de paradigme amène des opportunités, l'enjeu consiste à bénéficier des services cloud et de leurs avantages tout en assurant la souveraineté des institutions publiques et parapubliques, c'est-à-dire leur capacité d'autodétermination notamment sur l'utilisation des services cloud. Le fait que le marché des services cloud soit dominé par des entreprises américaines et chinoises d'un point de vue global présente un réel défi.

3.2.2. Sécurité et pérennité des données et de l'information durant tout le cycle de vie

L'utilisation de services cloud implique que les données transitent vers les infrastructures cloud du prestataire. Dans ce contexte, la sécurité du traitement et de la localisation des données, de la disponibilité du système et de l'accès aux données et au système doit être garantie. Mais l'utilisation d'un service n'est qu'une partie du cycle de vie du service ou système. Dans le contexte du décommissionnement – par exemple, en cas de défaillance du côté du prestataire – l'enjeu consiste à assurer à tout moment la restitution des données ou des services se trouvant dans le *cloud* par des services analogues ou des sauvegardes de données.

3.2.3. Impact environnemental

La mise à disposition de services cloud nécessite d'énormes ressources pour créer, exploiter et faire évoluer les infrastructures nécessaires à la technologie cloud. L'enjeu consiste à s'assurer que l'exploitant du *cloud* mette en place toutes les mesures possibles afin de diminuer l'empreinte écologique de son infrastructure, par exemple en utilisant des énergies renouvelables ou en recyclant les composants électroniques.

3.2.4. Marché local vs marché global

Le marché de prestataires *cloud* est très compétitif avec certains leaders internationaux qui sont très répandus, aussi bien dans le domaine professionnel que privé, et d'autres prestataires plus locaux, dont l'offre de services évolue rapidement (voir [3]). L'enjeu consiste pour les institutions publiques et parapubliques à trouver le bon équilibre entre des prestations cloud à forte valeur ajoutée qui peuvent se trouver sur le marché local, et celles reconnues et éprouvées issues des prestataires internationaux, ainsi qu'à profiter de l'innovation globale tout en promouvant l'attractivité de la place économique.

3.2.5. Compétences internes

L'utilisation de services cloud permet d'externaliser un certain nombre d'activités. Avec l'accélération de l'utilisation des services cloud, il convient de s'assurer de pouvoir disposer de ces compétences en suffisance lorsqu'une sortie du *cloud* est envisagée. Par ailleurs, le recours à des services cloud nécessite d'acquérir ou de renforcer certains profils tels que les juristes spécialisés dans les technologies de l'information pour la négociation et la contractualisation, et les ingénieurs système pour configurer et intégrer les services cloud avec les systèmes d'information des institutions publiques et parapubliques. L'enjeu consiste à acquérir les compétences et les profils nécessaires pour gérer et administrer les services cloud, tout en maintenant le contrôle sur les conséquences pour une administration (d'un point de vue organisationnel) et le savoir-faire en cas de sortie du *cloud*.

3.2.6. Marchés publics

En tant que pouvoir adjudicateur, l'entité publique est soumise à la législation sur les marchés publics pour les acquisitions de services cloud. Elle dispose d'une certaine liberté dans la définition de ses besoins et dans la configuration du marché. Elle est donc libre de choisir ce qui doit être réalisé et obtenu de la part des futurs soumissionnaires dans le cadre d'une procédure d'appel d'offres. Cette procédure a pour but de garantir une utilisation rationnelle des fonds publics mais œuvre également pour une concurrence saine par l'ouverture du marché. La configuration du marché ainsi que les besoins métiers identifiés doivent, en sus des dispositions relatives aux marchés publics, respecter les législations transversales comme la loi sur la protection des données ainsi que toutes les exigences liées au secret de fonction. Ces dernières ont pour conséquence, contrairement aux droits des marchés publics, de restreindre le périmètre du marché, notamment pour des motifs de sécurité de l'information et de dépendance, à de potentiels acteurs étrangers. L'adjudicateur devra donc faire en sorte d'harmoniser et de garantir la correcte application de diverses législations qui lui sont applicables et qui peuvent parfois paraître contradictoires. Ces exigences transversales se traduisent notamment par la mise en place de conditions de participation pouvant parfois aller à l'encontre de l'essence même de l'ouverture mutuelle des marchés. En effet, ces critères ont pour résultat de restreindre volontairement le marché à certains futurs soumissionnaires potentiels, qui ne pourraient pas être en mesure de garantir la bonne application des exigences de protection des données ou du secret de fonction.

Néanmoins, il est important de rappeler qu'il est formellement interdit de recourir à des spécifications techniques discriminatoires propres à tailler le marché sur mesure pour un soumissionnaire bien précis ou qui ont pour effet de pénaliser ou avantager certains soumissionnaires par rapport à d'autres sans justification. Dès lors, la complexité de l'élaboration du cahier des charges réside, pour le service métier de l'entité publique, dans l'harmonisation des diverses législations. De manière générale et en pratique, les règles concernant les marchés publics se révèlent difficiles d'application en ce qui concerne le domaine des technologies de l'information et notamment du *cloud*. Une réflexion politique et juridique au niveau national et régional (UE) pourrait être pertinente, dans l'optique d'une optimisation des règles dans ce domaine particulier.

3.2.7. For et droit applicable

Les éditeurs de solutions cloud susceptibles d'offrir des services à la mesure d'une entité publique font parfois partie d'entreprises situées à l'étranger. Cela entraîne une perte de maîtrise considérable ainsi qu'un enjeu de territorialité et de dépendance à des acteurs étrangers. Dès lors, des garde-fous doivent être mis en place lors du choix du fournisseur tant d'un point de vue juridique que politique. Dans tous les cas, il s'agit de préférer l'application du droit matériel suisse à un droit étranger ainsi qu'un for en Suisse, du point de vue de l'entité publique suisse. La décision de l'acceptation du risque de l'application d'un droit étranger et/ou d'un for à l'étranger doit être prise par le-la chef-fe de service. Dans la mesure du possible, il convient d'obtenir a minima un for alternatif (par exemple for du défendeur) et l'application du droit matériel suisse.

3.3. Cadre légal

Le recours à des services cloud génère beaucoup de questions juridiques, notamment du point de vue de la protection des données, du secret de fonction, de l'aspect contractuel et des règles relatives aux marchés publics.

L'appréhension de ce choix s'effectue également au travers du prisme de l'opportunité politique, stratégique et technique du point de vue de l'administration publique. Deux initiatives récentes mettent en évidence la complexité des aspects juridiques et les différentes approches et interprétations possibles.

Récemment, le Conseil d'État du Canton de Zürich a pris la décision d'autoriser son administration à déployer la solution en nuage Microsoft 365. Constatant que les solutions informatiques se développent toujours plus dans le nuage et qu'il devient de plus en plus difficile de s'en passer, le Conseil d'État zurichois a effectué une pesée des intérêts et a procédé à une évaluation des risques, en particulier au regard d'un potentiel accès aux données par des autorités étrangères. Sur la base des résultats obtenus, il considère que les risques liés à l'utilisation de la solution Microsoft 365 demeurent faibles et que le déploiement peut avoir lieu, moyennant notamment la création d'un poste de responsable de la sécurité du *cloud*.

La SUVA, souhaitant effectuer une démarche similaire, notamment à l'aide d'une analyse de risques d'un accès judiciaire aux données personnelles externalisées par une autorité étrangère, a soumis son analyse au Préposé fédéral à la protection des données et à la transparence (PFPDT). Le PFPDT rappelle en substance que l'admissibilité d'un transfert à l'étranger ou l'accès par une autorité étrangère ne repose pas sur une évaluation de risques, même si cette dernière reste un élément pertinent et intéressant pour qualifier les forces et faiblesses d'une externalisation. Dans le cas d'un transfert dans un pays n'offrant pas de niveau de protection adéquat, la question est de savoir si des garanties complémentaires suffisantes et effectives peuvent être mises en place.

Ces exemples (et les développements qu'ils contiennent) montrent que de nombreux éléments juridiques relatifs à l'utilisation de services en nuage ne sont pas encore tout à fait clairs ou qu'il n'existe pas encore de procédure standard.

Les thèmes abordés dans les exemples ci-dessus se concentrent sur les données transférées vers le *cloud*, leur stockage et leur transfert (souhaité / non souhaité) hors du territoire suisse. Dans les sections suivantes, les thèmes de la protection des données ainsi que le secret de fonction sont élaborés plus en détail[13].

3.3.1. Protection des données

Du point de vue de la protection des données, les lois cantonales de protection des données sont applicables à l'utilisation de services cloud, dans le cadre d'une externalisation effectuée par une entité publique cantonale. Le recours à la technologie cloud est principalement considéré comme une sous-traitance. Le responsable de traitement est l'entité publique et l'éditeur de la solution cloud, le sous-traitant. En général, si la relation entre l'entité publique et l'éditeur de la solution est de nature contractuelle, une base légale, ou à tout le moins une tâche publique, doit donner à l'éditeur la compétence de traiter les données personnelles concernées.

Aucune obligation légale ou contractuelle de confidentialité ne doit interdire le recours à la sous-traitance. En présence d'une telle obligation, le recours à une solution externalisée dans le *cloud*

[13] Les documents mis à disposition et considérés pour l'élaboration de cette étude sont listés ci-dessous (par ordre alphabétique) :

- Cedidac : Article de Nicolas Savoy, Mélanie Garcia, Ludivine Epiney, Catherine Pugin
- Laux Lawyers AG : Nuage public pour les services publics
- Privatim: Merkblatt Cloud-spezifische Risiken und Massnahmen
- Sylvain Métille : L'utilisation de l'informatique en nuage par l'administration publique
- Ville de Genève (15, Cours des Bastions Avocats Sàrl) : Note juridique – Office 365

n'est pas d'emblée exclu, mais une analyse de la licéité de la sous-traitance à l'aune de la disposition spéciale doit être effectuée, notamment en présence de secrets dits qualifiés. En outre, toutes les dispositions contractuelles, techniques et organisationnelles pertinentes doivent être prévues pour protéger les données soumises à un secret le cas échéant.

Il semble important d'aborder ici brièvement la notion de sous-traitant ultérieur ou de la sous-traitance dite « en cascade ». Concrètement, il s'agit de la situation d'un éditeur d'une solution cloud, soit le sous-traitant « primaire », qui fait appel à des sous-traitants qui lui sont propres pour fournir la prestation. Il s'agit, en soi, d'un risque supplémentaire en matière de protection des données qu'il convient d'intégrer rapidement dans la réflexion.

Il est d'ailleurs intéressant de constater que l'art. 9 al. 3 nLPD, prévoit que le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers qu'avec l'autorisation préalable du responsable de traitement. Il s'agit là d'une disposition dont la teneur est similaire à celle de l'art. 28 al. 2 du Règlement UE 2016/679 (RGPD).

Concrètement, afin de permettre au responsable de traitement d'effectuer un état des lieux et procéder à une analyse de risques, l'éditeur sous-traitant doit être en mesure de fournir une liste complète des sous-traitants ultérieurs engagés, notamment quant aux rôles de ces sous-traitants ultérieurs et de leur localisation. Le cadre contractuel doit prévoir a minima un rappel exprès que le sous-traitant « primaire » reste responsable des activités du sous-traitant ultérieur envers le responsable de traitement. En outre, un mécanisme de notification et d'approbation par le responsable de traitement en cas d'ajout ou de retrait d'un sous-traitant ultérieur doit être prévu dans le contrat avec l'éditeur sous-traitant.

S'agissant de la communication transfrontière, élément fréquemment rencontré dans le domaine du *cloud*, il convient de distinguer deux situations : le transfert vers et/ou l'accès depuis un pays offrant un niveau de protection adéquat, respectivement un pays n'offrant pas de niveau de protection adéquat.

Dans la première situation, aucune mesure supplémentaire n'est requise. Toutefois, le contrat de sous-traitance de protection des données doit régler les autres questions et assurer le respect des principes fondamentaux de la protection des données.

Dans le cas d'un transfert vers et/ou un accès depuis un pays n'offrant pas de niveau de protection adéquat, des mesures complémentaires sont nécessaires. Ces mesures peuvent prendre la forme de clauses contractuelles types (SCC – Standard Contractual Clauses) ou de règles d'entreprises contraignantes (BCR – Binding Corporate Rules). Toutefois, ces clauses sont par définition contractuelles et ne permettent pas une protection absolue et ne sauraient libérer l'entité publique de son devoir d'analyse de la situation. Un programme bilatéral de type Swiss – US Privacy Shield pourrait permettre de transférer des données dans un pays n'offrant pas un niveau de protection adéquat. Cependant, l'accord similaire UE – US Privacy Shield a été invalidé par la CJUE en 2020 et le PFPDT recommande de ne plus se baser sur ce type de système, même si la décision européenne n'est pas applicable en Suisse. La Commission européenne et les Etats-Unis travaillent actuellement sur un « Trans-Atlantic Data Privacy Framework » pour remplacer le Privacy Shield ; la Suisse devrait en principe convenir d'un accord similaire dans les temps à venir.

Il convient de souligner que l'appréciation politique ou stratégique peut s'opposer à tout transfert vers et/ou accès depuis l'étranger, même si le pays de destination ou d'accès offre un niveau de protection adéquat, ou dans le cas de mesures complémentaires satisfaisantes si le niveau de protection offert par le pays de destination n'est pas suffisant.

3.3.2. Secret de fonction

Les collaborateurs de la fonction publique ou le délégataire de la fonction publique ont l'interdiction de divulguer des informations ou des documents officiels dont ils ont eu connaissance dans l'exercice de leur fonction et qui doivent rester secrets en raison de la loi ou d'un intérêt public ou privé prépondérant. La violation du secret de fonction est dans ce sens sanctionnée par l'art. 320 CP.

Pour être punissable, la divulgation d'une information protégée par un secret doit se faire envers une personne non autorisée. Dès lors, en matière de *cloud*, il s'agit de déterminer si l'éditeur, généralement qualifié de sous-traitant en matière de protection des données, peut être considéré comme un auxiliaire du détenteur du secret de fonction, par analogie à ce qui est prévu pour le secret professionnel (art. 321 CP). Il convient de préciser que le Tribunal fédéral considère que l'obligation de tenir le secret n'a pas besoin d'être inscrite dans une loi au sens formel. L'art. 320 CP englobe tous les secrets confiés à un fonctionnaire ou dont il a pris connaissance en raison de sa fonction, indépendamment de savoir si une norme spéciale l'oblige à garder le secret. Toutefois, une modification de l'art. 320 CP, attendue pour 2023, prévoira expressément la notion d'auxiliaire du secret et s'appliquera vraisemblablement à un éditeur d'une solution cloud offerte à une entité publique détentrice du secret.

Si cet éclaircissement est bienvenu, la question du secret de fonction dans le cadre d'une communication transfrontière reste ouverte. En effet, si l'éditeur auxiliaire du secret de fonction est étranger (et soumis à un droit étranger) ou si les données soumises au secret se trouvent à l'étranger, il semble difficile d'opposer une norme de droit suisse à une requête officielle et valable d'une autorité étrangère sur son territoire et de sanctionner cette entité de l'éditeur sise à l'étranger.

Le chiffrement des données pourrait apporter une réponse à cette problématique, si l'éditeur *cloud* ne possède pas la clé de chiffrement et qu'il n'a aucune possibilité d'accéder aux données en clair ; Il n'y aura pas de violation du secret de fonction dans ce cas, même en cas d'hébergement à l'étranger.

Afin de réduire le risque, des garanties contractuelles avec l'éditeur *cloud* doivent être implémentées. En premier lieu, ce dernier doit s'engager à n'accéder aux données que lorsque cela est strictement nécessaire à l'exécution de la prestation. Ensuite, en fonction du secret et des risques en jeu, les collaborateur-trice-s de l'éditeur peuvent être tenu-e-s de signer un accord de confidentialité avec rappel des enjeux sur cette problématique.

Le contrat peut également prévoir des peines conventionnelles suffisamment sévères et dissuasives afin de limiter le risque de violation du secret par l'éditeur.

Enfin, il appartient au service métier bénéficiaire de l'entité publique d'effectuer un état des lieux et une analyse de risques concernant cette problématique. En effet, c'est le service bénéficiaire qui a la connaissance et la compétence s'agissant de l'appréhension de ses propres règles sectorielles.

3.3.3. Synthèse et référence à d'autres analyses

Dans le contexte de l'utilisation de services cloud par une administration, les éléments suivants doivent être pris en considération :

- Bases légales :
  L'entité publique s'assure d'avoir les bases légales pertinentes pour le traitement de données personnelles dont l'externalisation est envisagée. Ces bases légales précisent les contours du traitement de données et seront utiles dans le choix et le périmètre de l'externalisation.
- Sous-traitance ultérieure :
  L'entité publique s'assure que les propres sous-traitants de l'éditeur (sous-traitants dits « ultérieurs ») permettent à la première d'être conforme à ses obligations en matière de protection des données. L'entité publique doit pouvoir en avoir une vision claire sur les activités concernées et sur d'éventuels transferts internationaux par ce biais.
- Transferts et accès aux données :
  Dans le cas d'un transfert vers et/ou un accès depuis un pays n'offrant pas de niveau de protection adéquat, des mesures et des analyses complémentaires seront nécessaires.

- Contrat de sous-traitance de protection des données :
  Un contrat de sous-traitance de protection des données, entre l'entité publique et l'éditeur sous-traitant complète le cadre contractuel (contrat commercial, SLA, etc.) en établissant les droits et obligations des parties en la matière. Un soin particulier est amené à la hiérarchie de ces documents, aux obligations d'annonces en cas d'incidents de sécurité, d'audit des autorités cantonales de contrôles (Cours des comptes, Préposé à la protection des données, etc.) et aux modalités de sortie.
- Situations intercantonales ou fédérales :
  Dans l'éventualité d'une mutualisation des ressources entre plusieurs cantons et/ou communes et/ou avec la confédération, une analyse en matière de bases légales, de protection des données, de droit applicable, de financement, de responsabilité et de gouvernance est menée par les parties prenantes et concrétisée, le cas échéant, dans une convention.
- Secret de fonction :
  Le secret de fonction n'empêche pas d'emblée tout recours à des sous-traitants. L'entité publique évalue la situation et effectue, le cas échéant, une analyse de risques. En fonction des résultats, toutes les dispositions contractuelles, techniques et organisationnelles pertinentes devront être prévues pour protéger les données soumises à un secret le cas échéant, notamment par l'implémentation de peines conventionnelles sévères. Une levée du secret par l'autorité supérieure peut être envisageable en ultima ratio.

En résumé, dans ce contexte, les cantons doivent encore relever certains défis en matière d'utilisation des services cloud. Toutefois, si des mesures suffisantes sont mises en place pour les cas considérés, aucun obstacle juridique incontournable ne s'oppose à la migration vers le *cloud*.

4. La souveraineté numérique sous un angle technique

Avec la montée en puissance du *cloud*, les technologies de développement et de fourniture de service et de systèmes modernes d'eGovernment ont changé. Par conséquent, l'exploitation des technologies change également et, avec elle, la gouvernance. Comme décrit ci-dessus, cela présente plusieurs avantages, car de nombreuses tâches[14] tout au long du cycle de vie du système ou du service peuvent être déléguées et le contrôle de l'infrastructure est ainsi confié à ceux qui sont experts en la matière. Mais, en cédant ces tâches, la maîtrise complète est également abandonnée. Une administration cantonale qui a abandonné ce contrôle est-elle encore souveraine ? Ou plus spécifiquement : à partir de quand n'est-elle plus « suffisamment » souveraine ?

Ce chapitre fait une proposition de définition de cet aspect de souveraineté dans le domaine du numérique.

Afin de simplifier la lecture, le terme « système » est utilisé pour couvrir les deux notions : d'une part, celui d'un système informatique (application, software, hardware, réseaux d'accès, routage, serveur, etc.) et d'autre part, celui d'un service numérique en général.

4.1. Définition de la souveraineté numérique

La notion de la souveraineté numérique fait l'objet d'un regain d'intérêt dans les milieux scientifiques et politiques et un débat a vu le jour sur le maintien et le renforcement de la souveraineté numérique en Europe. En raison de la pertinence actuelle du thème et du débat qu'il suscite, un grand nombre de documents se penchent sur la discussion théorique de la souveraineté numérique. Le ministère à l'économie et à l'énergie d'Allemagne (BMWi) présente une vue consolidée d'une longue liste de résultats et de définitions (voir [4]), utilisée comme référence dans cette étude. Jusqu'à présent, aucune définition de la souveraineté numérique ne s'est imposée.

L'objectif de ce chapitre est d'établir des définitions de travail pour ces termes largement utilisés dans les milieux scientifiques et politiques. Ces définitions ne sont pas immuables et seront enrichies par les résultats de l'étude académique (voir [2]), mais servent comme base de discussion et de réflexion pour la présente étude. Les définitions se basent et résultent de consolidations des définitions utilisées dans différents projets suisses et européens pertinents (voir documents en annexe).

Définition de la souveraineté numérique :

La souveraineté numérique est la capacité d'autodétermination d'une entité (légale) en ce qui concerne tout le cycle de vie d'un système numérique, de la conception jusqu'au décommissionnement, en passant par l'utilisation de systèmes numériques et des données qui sont traitées et stockées ainsi que des processus qu'ils représentent.

Cette définition permet de prendre en compte tous les aspects pertinents d'un service numérique en considérant toutes les conditions-cadres et tout en restant agnostique à la technologie. Ceci est pertinent dans la mesure où la technologie évoluera toujours et rapidement et que la souveraineté devrait en principe pouvoir être satisfaite par n'importe quelle technologie – que cela soit de l'IoT industrielle, du *cloud* ou autres.

De plus cette définition s'applique également à la notion de la souveraineté des données. La souveraineté des données est définie comme la capacité d'autodétermination en ce qui concerne tout le cycle de vie des données propriétaires et des données qui sont créés. La souveraineté des données est alors une partie intégrale et nécessaire de la souveraineté numérique, mais **n'est pas identique**. En effet, là où la souveraineté numérique définit le niveau d'autodétermination sur les technologies de l'information et de la communication de manière générale, la souveraineté des

[14] Les tâches correspondent entre autres aux tâches de gestion liées aux dimensions identifiées dans le Tableau 1.

données en est un sous-ensemble. Ce dernier considère la souveraineté sur l'aspect des données, notamment leur transfert, leur stockage, leur traitement et leur effacement.

Il convient de noter que cette définition permet des niveaux intermédiaires de souveraineté (et pas seulement des extrêmes avec ou sans souveraineté). Cela est nécessaire pour pouvoir distinguer les systèmes pour lesquels une entreprise ou une administration est autodéterminée à certains égards, mais pas à d'autres. Dans les dimensions présentées ci-après, il est également précisé que les systèmes informatiques sont constitués généralement de nombreux composants ou sous-systèmes individuels et qu'il convient ici aussi de différencier les cas dans lesquels un système est souverain de ceux dans lesquels il ne l'est pas.

4.2. Contexte politique « stable » et de « crise »

Les administrations publiques utilisent des systèmes qu'elles ont soit développés elles-mêmes, soit commandés ou achetés directement auprès de fournisseurs – elles dépendent donc dans de nombreux cas de fournisseurs. Ces derniers, qui sont d'une part propriétaires de ces systèmes et d'autre part les développent et les exploitent en tant que services, doivent constamment les faire progresser afin de garantir la valeur ajoutée pour leurs clients. Les conditions-cadres à cet effet diffèrent d'un fournisseur à l'autre : non seulement les facteurs technologiques jouent un rôle essentiel, mais la situation économique, politique et juridique du pays impacte également l'entreprise.

Il en résulte une complexité accrue des facteurs qui influencent la collaboration entre l'administration publique et ses fournisseurs. Pour contrôler cette dépendance et cette complexité, ainsi que pour minimiser les risques tout en permettant la coopération et une autodétermination par une administration, il faut mettre en place des contrats.

Dans cette étude, deux contextes extrêmes sont considérés : d'un côté le contexte politique « stable » et de l'autre, le contexte politique en « crise ».

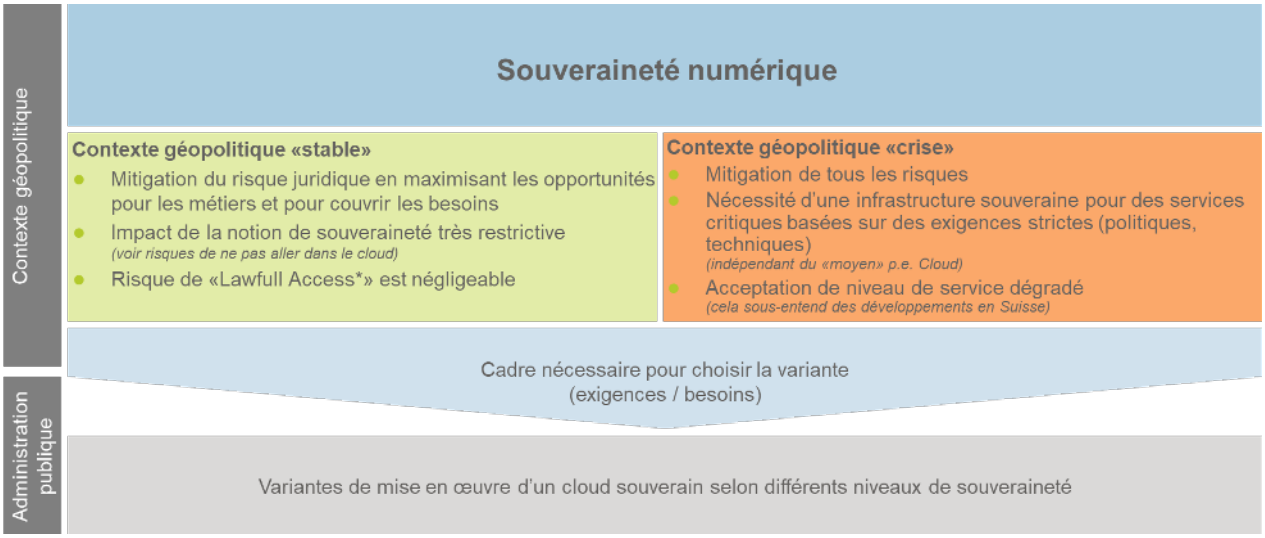

Figure 1: Souveraineté selon les contextes géopolitiques

4.2.1. Contexte géopolitique « stable »

Dans le contexte géopolitique « stable », il peut être supposé que toutes les parties contractantes (administration publique, fournisseur et sous-traitant) respectent les contrats et que les organes juridiques peuvent exécuter leur mission. Le besoin d'une souveraineté accrue est limité, car la confiance dans le fait que les services seront fournis comme convenu est élevée. Les opportunités pour les métiers et leurs besoins peuvent être maximisées.

La souveraineté numérique en général ne doit pas être particulièrement élevée dans ce contexte. Les risques juridiques doivent être mitigés mais une souveraineté trop élevée aurait un effet contraignant, qui n'est pas pertinent en relation avec les risques, entre autres de « Lawful Access ».

Pour la suite de cette étude, les réflexions sont faites dans la considération d'un contexte géopolitique « stable », malgré la situation politique actuelle en Europe. Dans un contexte de crise (chapitre 4.2.2), les risques ne sont pas prévisibles et ne peuvent pas être expliqués rationnellement.

4.2.2. Contexte géopolitique « crise »

Dans le contexte géopolitique de « crise », par exemple en cas de conflit politique, tous les risques possibles doivent être mitigés. Les administrations publiques doivent pouvoir livrer leurs services critiques dans toutes les circonstances et ont donc besoin d'une infrastructure entièrement souveraine – la souveraineté numérique doit donc être à un niveau élevé pour la majorité des dimensions. Pour cela, les services critiques doivent être identifiés et des exigences strictes (aux niveaux technique et politique) doivent être définies. Cela sous-entend des développements propres ou par le recours à des fournisseurs particulièrement fiables. Ces exigences ont un impact très restrictif sur le niveau de service qui, dans ce contexte de crise, peut être dégradé.

Le passage d'un contexte stable à un contexte de crise nécessite une préparation minutieuse, afin que celui-ci puisse être effectué de manière contrôlée dans chaque situation. Il s'agit également d'un élément essentiel de la souveraineté numérique – à tout moment, l'organisation doit pouvoir déterminer elle-même quels services elle utilise et comment. Ce passage nécessite différents plans, notamment un plan de reprise après sinistre (desaster recovery plan) et un plan pour la migration vers les systèmes hautement souverain.

Pour la suite de cette étude, la situation de « crise » est mise hors périmètre. Celle-ci doit cependant être traitée à l'avenir afin de garantir la souveraineté numérique en tout temps.

4.3. Les dimensions de la souveraineté numérique pour les systèmes d'information

Dans le cadre de cette étude, douze dimensions ont été identifiées afin de préciser la souveraineté numérique d'un système. Ces dimensions peuvent être regroupées en trois catégories, couvrant ainsi le cycle de vie d'un système et de conditions-cadres qui doivent être remplies pour garantir la souveraineté.

Les dimensions pour la souveraineté numérique développées dans le cadre de cette étude sont présentées ci-dessous. Les dimensions du cycle de vie sont listées en vert et celles des conditions-cadres en bleu. Les différentes dimensions sont détaillées dans les sections suivantes.

Catégorie		Dimension	La **souveraineté numérique** est remplie quand l'administration cantonale…
Cycle de vie d' un système	Création / évolution	Développement du système	… a la possibilité de gouverner ou de maitriser le développement, l'intégration et l'évolution du système
		Durabilité	… a la possibilité de gouverner ou de maitriser les aspects de durabilité de la solution
	Utilisation	Traitement des données	… a la possibilité de choisir où (systèmes) et comment les données sont traitées
		Localisation des données	… a la possibilité de choisir où (géographie) les données sont localisées lors de leur traitement, transport et stockage
		Disponibilité du système	… a la possibilité d'accéder et d'utiliser le système à tout moment
		Accès au système et aux données	… a la maitrise sur l'accès (libération et suivi des accès d'utilisateurs, d'administrateurs et de systèmes) aux données et contrôle la chaîne de support (y compris prestataires)
		Gestion de l'évolution	… a la possibilité de décider si une nouvelle version / une nouvelle licence / une conséquence technologique, financière ou organisationnelle est acceptée et à quel moment
	Décommissionnement	Stratégie exit[15]	… a la possibilité en termes de moyens financiers, de savoir-faire et de compétences décisionnelles pour changer de solution sans désavantages majeurs
		Extraction des données	… a la possibilité en termes de formatage, standard ou interface d'extraire toutes ses données ou de les détruire et de confirmer ou prouver leur destruction
Conditions-cadres		Cadre juridique	… ainsi que les systèmes utilisés sont conformes avec le cadre juridique et sont soumis à des lois extraterritoriales d'autres pays
		Expertise	… a accès (sur son territoire) au savoir-faire et à l'expertise nécessaire tout au long du cycle de vie
		Contrats	… peut mettre en place des contrats qui couvrent toutes les exigences et a la possibilité de les adapter pour tout changement d'exigence

Tableau 1: Dimensions de la souveraineté numérique pour un système d'information

4.3.1. Différents niveaux de souveraineté par dimension

Un niveau d'autodétermination peut être défini pour chaque dimension de la souveraineté numérique. D'une manière générale, un niveau d'autodétermination plus élevé dans une dimension signifie plus de contrôle et d'autonomie, mais potentiellement plus de prise de responsabilité et d'efforts (financiers, organisationnels, savoir-faire). En revanche, un niveau plus bas signifie une externalisation vers des partenaires spécialisés, la possibilité de se spécialiser dans l'activité principale, mais aussi une perte d'autonomie et une dépendance.

En principe, de nombreux niveaux intermédiaires sont envisageables, mais une focalisation sur quelques niveaux permet de mieux cibler la discussion. Les niveaux sélectionnés à cet effet sont présentés ci-dessous. Cette section donne un aperçu des trois niveaux différents – 1 (faible souveraineté) à 3 (souveraineté élevée) – que peut prendre chaque dimension. Ces niveaux sont indicatifs et peuvent varier en fonction de la situation spécifique rencontrée – l'accent est mis ici sur la comparaison plutôt que sur une mesurabilité de la souveraineté.

[15] La stratégie d'exit décrit la stratégie ultime de réduction des risques lorsque l'organisation met fin à la consommation d'un service d'un prestataire externe. Il peut s'agir de la sortie et de la transition des fonctions et des données externalisées vers un autre fournisseur (en partie ou en totalité), du retour de ces fonctions sur site (*on-premise*), ou de l'arrêt du processus.

Il convient de noter qu'en raison de la présence de ces dimensions étendues, il n'existe manifestement plus une seule définition de « souveraineté » ou de « non-souveraineté » pour un service.

Le **niveau 1** pose des exigences de base en matière de souveraineté, qui peuvent généralement être attendues des systèmes.

Le **niveau 2** se réfère à des exigences avancées en matière de souveraineté, notamment en ce qui concerne la criticité accrue d'un système ou l'existence d'exigences spécifiques en matière de contrôle reçu.

Le **niveau 3** pose des exigences élevées en matière de souveraineté, qui peuvent également aller jusqu'au contrôle et à l'autonomie complets sur les différents aspects du cycle de vie et/ou du cadre du système.

Un niveau 0, ne posant aucune exigence envers la souveraineté, est également envisageable mais est omis de cette étude. Chaque augmentation du niveau répond à une exigence spécifique envers un système. En effet, un niveau de souveraineté plus élevé exige un effort en ressources en termes d'expertise propre et de développement et opération du système. Ça serait donc irréaliste en raison des coûts élevés, du rythme plus lent de l'innovation et de la complexité des chaînes d'approvisionnement mondiales existantes dans de nombreux domaines. Un niveau de souveraineté plus bas exige en revanche souvent un plus grand effort de gestion et de coordination avec les fournisseurs de services et une expertise dans l'interaction entre les systèmes. La souveraineté numérique a besoin d'un équilibre viable entre le pragmatisme lié aux réalités du marché et aux mécanismes d'interdépendance – sur lesquels s'est construit le numérique – et une pleine capacité d'action.

Le tableau ci-dessous donne un aperçu des niveaux choisis pour chaque dimension[16].

[16] Il convient de noter à nouveau ici que le niveau de souveraineté choisi représente seulement un ordre de grandeur.

Catégorie		Exigences standard de souveraineté numérique par dimension		
		Niveau 1	Niveau 2	Niveau 3
Cycle de vie	Création / évolution	Développement du système		
		Pas de contrôle direct sur le développement et l'évolution, mais exigence de certifications et / ou audits correspondant(e)s par des tiers dûment approuvés	Influence dans le développement et l'évolution, exigence de certifications et / ou audits correspondant(e)s possibles par des tiers dûment approuvés	Contrôle direct sur le développement et l'évolution du système
		Durabilité		
		Pas de contrôle direct sur la durabilité du système, mais exigence de certifications et / ou audits correspondant(e)s possibles par des tiers dûment approuvés	Influence sur la durabilité du système, exigence de certifications et / ou audits correspondant(e)s possibles par des tiers dûment approuvés	Contrôle direct sur la durabilité du système
	Utilisation	Traitement des données		
		Les systèmes inclus dans la chaîne de traitement et de stockage ne sont pas strictement identifiés ou contrôlés	Les systèmes inclus dans la chaîne de traitement et de stockage sont connus ou contrôlés	Les systèmes inclus dans la chaîne de traitement et de stockage sont sous le contrôle du commanditaire
		Localisation des données		
		Le traitement et le stockage des données ne sont pas limités géographiquement, mais pourraient être configurés sur le plan technique ou organisationnel (contractuel)	Les données sont traitées et stockées en Suisse, certaines (p. ex. données d'identité) en UE	Les données sont traitées et stockées en Suisse, sur des systèmes de stockage contrôlés par le commanditaire
		Disponibilité du système		
		La disponibilité du système peut être contrôlée ou influencée par les choix architecturaux et est vérifiable de bout en bout grâce aux outils mis à disposition	La disponibilité du système est contrôlée par les choix architecturaux et est directement vérifiable de bout en bout par l'organisation	Tous les systèmes, et donc aussi leurs disponibilités, sont sous contrôle du commanditaire
		Accès au système et aux données		
		Chaque accès est autorisé par le propriétaire des données et est vérifiable à tout moment	Chaque accès est autorisé par le propriétaire des données et est vérifiable à tout moment, la chaîne de support est strictement contrôlée	Chaque accès est autorisé par le propriétaire des données grâce à des processus et systèmes sous contrôle du commanditaire
		Gestion de l'évolution		
		Les modifications fonctionnelles ou financières sur les systèmes non gérés par le commanditaire sont effectuées sur la base des spécifications du fournisseur	Assurance que toute modification fonctionnelle ou financière du système ne sera mise en œuvre qu'après un délai convenu contractuellement	Toute modification fonctionnelle ou financière du système est contrôlée par le commanditaire (au maximum techniquement possible)

Catégorie		Exigences standard de souveraineté numérique par dimension		
		Niveau 1	Niveau 2	Niveau 3
Cycle de vie	Décommissionnement	Stratégie exit		
		Il est envisageable et possible de changer de système après un délai donné et à des coûts acceptables (organisationnels, financiers, savoir-faire)	Le système est concevable (p. ex. architecture, infrastructure) de façon à minimiser les coûts (organisationnels, financiers, savoir-faire) pour changer de système	Le système est conçu (p. ex. architecture, infrastructure) par le commanditaire et le changement de système est contrôlé par le même
		Extraction des données		
		Les données propriétaires peuvent être extraites et/ou détruites lors d'un exit, suppression confirmable sur le plan organisationnel (selon possibilités légales)	Les données propriétaires peuvent être facilement extraites et/ou détruites lors d'un exit, suppression prouvable sur le plan technique (selon possibilités légales)	Le système est contrôlé par le commanditaire et l'extraction et/ou la destruction des données propriétaires aussi (selon possibilités légales)
Conditions-cadres		Cadre juridique		
		Le cadre juridique du commanditaire est entièrement respecté	Le cadre juridique est défini par le commanditaire (dans la mesure du possible) et est pleinement respecté	Le cadre juridique ne concerne que le commanditaire ou est défini par lui de manière significative (dans la mesure du possible) et est entièrement respecté
		Expertise		
		Le minimum de savoir-faire et de ressources pour gérer le système ou les partenaires sont disponibles en interne chez le commanditaire	Le commanditaire dispose d'un savoir-faire et de ressources suffisantes pour surveiller et influencer le cycle de vie du système	Le cycle de vie du système repose en grande partie sur le savoir-faire et les ressources du commanditaire
		Contrats		
		Les contrats couvrent les exigences du système, de sa sécurité et sa souveraineté mais ne sont adaptables qu'à plus grands efforts pendant le cycle de vie du système	Les contrats couvrent les exigences du système, de sa sécurité et sa souveraineté et peuvent être adaptés selon l'évolution des besoins après un délai prédéfini	Le fournisseur agit pour le compte et dans l'intérêt direct du commanditaire, les contrats (si existants) sont facilement adaptables

Tableau 2: Exigences standard de souveraineté numérique par dimension

4.4. Labélisation

Différentes administrations publiques ont élaboré des référentiels[17] permettant la qualification de prestataires et de leurs services cloud, avec l'objectif de promouvoir l'offre des prestataires dit « de confiance ». L'approche de labélisation par une entité centrale permet de traiter la problématique de la sécurité de manière globale et efficace, favorisant l'émergence de services qualifiés. Les prestataires disposent d'un cadre et des exigences pour se faire qualifier et pour les consommateurs (publics ou privés) pouvant fonder leur confiance sur cette qualification. Les référentiels sont basés sur des exigences techniques et organisationnelles pour les aspects de sécurité, d'hébergement et de traitement des données dans le pays ou dans le territoire européen.

[17] « SecNumCloud » de l'Agence nationale de la sécurité des systèmes d'information (République Française) ; « European Secure Cloud » de l'Agence nationale de la sécurité des systèmes d'information (République Française) et le BCI Allemand

Le contenu de ces référentiels se recoupe dans certaines des douze dimensions identifiées dans cette étude. Il s'agit principalement des dimensions « Traitement des données », « Localisation des données » et « Cadre juridique », ainsi que d'aspects de sécurité explicites dans plusieurs dimensions. Il convient de noter que les exigences dans ces référentiels ont un objectif différent, à savoir la cybersécurité.

Cette approche de référentiel peut être appliquée à la souveraineté numérique. Sur la base de standards existants et nouveaux, il est possible d'établir des exigences qui couvrent toutes les dimensions mentionnées dans le chapitre précédent. Cela permettrait également de clarifier la terminologie et de favoriser le dialogue et la compréhension générale de la souveraineté numérique. Ce référentiel peut être utilisé pour gagner en expérience et maturité et, avec l'aide d'un mécanisme de labélisation, à évaluer le marché en termes de souveraineté. Ensuite ce référentiel peu évoluer vers une ou plusieurs normes dominantes dans la thématique de la souveraineté numérique dans le *cloud* et elles peuvent être utilisées pour des certifications.

5. Le cloud souverain

Cette section se penche sur la déclinaison de la souveraineté numérique appliquée au *cloud* et sur les variantes possibles de mise en œuvre répondant à des exigences de souveraineté.

5.1. Cloud dans le contexte de la souveraineté numérique

Le chapitre 4 décrit les dimensions de la souveraineté numérique. Il établit la souveraineté d'un système générique, car les systèmes informatiques se composent de nombreux sous-systèmes qui sont couplés entre eux dans un but précis. Pour qu'un système soit jugé souverain, il doit donner un degré de confiance suffisant dans les éléments qui le sous-tendent. Il est donc souverain si les éléments qui le sous-tendent (y compris les entreprises associées, les collaborateurs et les sous-traitants) peuvent fournir un même niveau de souveraineté (ou un niveau plus élevé). Si ce n'est pas le cas, il devient alors difficile de fournir des garanties sur la souveraineté du système dans son ensemble.

Définition du cloud souverain :

Un *cloud* est (suffisamment[18]) souverain si les systèmes considérés de l'entité (légale) qui l'utilise donnent à cette dernière la capacité (suffisante) d'autodétermination sur l'ensemble du cycle de vie, y compris la conception/l'évolution, l'utilisation et le décommissionnement des systèmes utilisés et des données qu'ils traitent et stockent, ainsi que des processus qui les soutiennent.

Pour valider qu'un *cloud* est souverain, il faut considérer tous les niveaux de la pile matérielle, logicielle et contractuelle qui le constituent et les exigences envers la souveraineté qui y sont déduites. Il est possible de se baser sur la classification des données en fonction de leur criticité et sensibilité et ensuite de considérer les exigences techniques, procédurales et organisationnelles en matière de cybersécurité, de sécurité des données et de contrôle attendu sur les différents sous-systèmes, qui composent le système global.

En résumé, la souveraineté d'un *cloud* est toujours liée aux exigences définies. La question à se poser dès lors pour une administration cantonale est la suivante : quel est le niveau de souveraineté minimal requis pour un système donné, sur la base des exigences définies ? Si une solution cloud offre un niveau suffisant par dimension, elle peut être qualifiée de « suffisamment souveraine »[19].

Ce raisonnement implique donc qu'il ne peut pas y avoir de définition unique d'un cloud souverain ou, en d'autres termes, qu'il n'y a pas d'exigences clairement définies envers le niveau de souveraineté pour un service cloud pour le qualifier de « souverain ».

[18] Comme il n'y a pas de niveau de souveraineté unique et qu'il n'y a pas de seuil unique à partir duquel un cloud ne serait plus souverain, l'étude réfère à une souveraineté « suffisante ».

[19] Il s'agit de rappeler que les niveaux (1,2,3) de souveraineté sont indicatifs, dans le sens qu'il existe une gradation continue.

5.2. Consommation d'un service cloud à travers un broker

Un broker est une entité publique ou privée qui gère l'utilisation, la performance et la mise à disposition de services cloud, et qui négocie les relations entre les fournisseurs et les consommateurs de service cloud. À mesure que le *cloud computing* évolue, l'intégration des services cloud peut devenir trop complexe pour que les consommateurs de *cloud* puissent la gérer seuls. Dans de tels cas, un consommateur peut demander des services cloud chez le broker, au lieu de contacter directement un fournisseur et il devient le client du broker.

Dans le cadre de cette étude et des variantes développées ci-dessous le rôle du broker peut être pris en charge par une entité privée ou par une entité publique existante ou créée à cet effet. Dans les deux cas de la consommation de service cloud à travers un broker privé ou public, le niveau de souveraineté n'augmente pas considérablement pour une administration publique. En termes de dimension de souveraineté, comme présenté dans le chapitre 4.3, le broker amène des avantages dans les dimensions suivantes : la gestion de l'évolution, la stratégie exit, l'extraction des données, le cadre juridique, l'expertise et les contrats.

Dans les deux cas (broker public ou privé), les facteurs décisifs sont la collaboration entre le broker et l'administration cantonale ainsi que l'expertise du broker.

Les avantages de la consommation de services cloud à travers un broker peuvent inclure :

- La disponibilité des services cloud est élevée, grâce aux potentiellement multiples fournisseurs derrière le broker et à la dépendance réduite à l'égard d'un seul fournisseur
- L'amélioration des accords de niveau de service (SLA) en exploitant plusieurs fournisseurs de services cloud et la scalabilité
- La réduction des coûts – remises importantes sur les volumes en cas d'achat d'un grand nombre de services
- Pour chaque « client » du broker, l'effort individuel pour la consommation de service cloud est réduit
- La génération de plus-value grâce à l'expertise du broker

Les désavantages de la consommation de services cloud à travers un broker peuvent inclure :

- La dépendance de l'organisation à l'égard du broker pour être continuellement à jour sur les nouvelles technologies, options et offres de *cloud*
- Le recours à un broker rend également plus complexe le maintien des exigences de sécurité d'une organisation tout au long de la chaîne de livraison, car le broker ajoute une couche entre les fournisseurs de services et l'organisation
- Il existe des conflits d'intérêts potentiels[20], de sorte que l'organisation doit s'assurer que le broker agit constamment dans l'intérêt de son client lorsqu'il recommande des offres de *cloud computing*.

Il existe différentes options pour les services de brokering internationaux et nationaux dans un environnement privé[21]. En règle générale, les entreprises qui fournissent leurs propres services cloud ou a minima des offres de développement sur des services cloud proposent également un service de broker à plus ou moins grande échelle. Lors de la sélection d'un broker, il convient dans tous les cas de tenir compte de la forme de collaboration souhaitée, du cadre contractuel et, en général, du respect des exigences basées sur la souveraineté souhaitée selon la variante choisie.

---

[20] Le broker poursuit des objectifs de gestion d'entreprise. Il y a donc d'une part un conflit d'intérêts dans la valorisation du service offert par le broker : le consommateur, c'est-à-dire l'administration cantonale, ne profitera pas de la même manière d'un changement de prix du service par le fournisseur que d'autres clients, par exemple. D'autre part, le broker offre des services non-ciblés qui servent à tous ses clients et qui ne correspondent potentiellement pas aux services spécifiques souhaités par l'administration cantonale.

[21] Petits ou grands prestataires de services informatiques, locaux ou internationaux, qui offrent des services d'exploitation et/ou de managed services sur des infrastructures en partie propres, mais aussi en particulier sur des infrastructures cloud de prestataires tiers. Voir l'étude de marché [3] pour plus de détails.

5.3. Variantes de cloud répondant à un niveau de souveraineté spécifique

Ce chapitre décrit les différentes variantes de mise en œuvre d'un *cloud* répondant à un niveau de souveraineté[22]. Les variantes se déclinent en plusieurs sous-variantes afin d'illustrer les aspects différenciateurs de manière plus compréhensible. Il convient de noter dès à présent que les différentes variantes ne s'excluent pas mutuellement, mais qu'il est possible de combiner des variantes en fonction du cas d'usage considéré.

Figure 2: Vue d'ensemble des variantes de cloud répondant à un niveau de souveraineté spécifique.

[22] Les variantes dans lesquelles un niveau de souveraineté de base n'est pas atteint ne sont pas considérées dans cette étude.

5.3.1. *Types variantes 1 | Service Cloud « sur étagère »*[23]

Variante 1a : Le métier achète un service standard sans fortes adaptations pour sa propre consommation ou l'IT l'achète pour le mettre à disposition du métier.

Exemple : Service de traduction deepl.com acquis[24] *et exploité directement par un département métier interne.*

Variante 1b : L'IT engage un broker privé ou public pour mettre un service standard à disposition du métier et de l'IT.

Exemple : Service de traduction deepl.com acquis et exploité par un prestataire de services IT du canton ou une entreprise privée spécialisée (broker).

L'objectif de ces variantes est de répondre à un cas d'usage en consommant un service *« sur étagère »* d'un fournisseur de prestations *cloud* de ce type et de maximiser la simplicité de l'achat et de l'exploitation, en s'appuyant intégralement sur les technologies et services des fournisseurs (par exemple un *hyperscaler*). Ce type de variantes est défini par l'utilisation des systèmes tels qu'ils sont fournis, avec une configuration minimale de la part du commanditaire. Ces variantes couvrent un niveau de base des exigences de souveraineté.

Ce service peut être directement acheté par l'utilisateur final ou peut être mis à disposition par l'IT (variante 1a) de l'administration cantonale. Ce service peut également être consommé à travers un broker privé ou public (variante 1b).

Degré de souveraineté atteignable par dimension des variantes de type 1[25]

			Niveau 1	2	3	Exigences standard de souveraineté numérique
Cycle de vie	Création/ évolution	Développement du système	●			Pas de contrôle direct sur le développement et l'évolution, mais exigence de certifications et / ou audits correspondant(e)s
		Durabilité	●			Pas de contrôle direct sur la durabilité du système, mais exigence de certifications et / ou audits correspondant(e)s possibles
	Utilisation	Traitement des données	●			Les systèmes inclus dans la chaîne de traitement et de stockage ne sont pas strictement identifiés ou contrôlés
		Localisation des données	●	○		Le traitement et le stockage des données ne sont pas limités géographiquement, mais pourraient être configurés sur le plan technique ou organisationnel (contractuel)
		Disponibilité du système	●	○		La disponibilité du système peut être contrôlée ou influencée par les choix architecturaux et est vérifiable de bout en bout grâce aux outils mis à disposition
		Accès au système et aux données	●	○		Chaque accès est autorisé par le propriétaire des données et est vérifiable à tout moment
		Gestion de l'évolution	●	○		Les modifications fonctionnelles ou financières sur les systèmes non gérés par le commanditaire sont effectuées sur la base des spécifications du fournisseur
	Décommissionnement	Stratégie exit	●			Il est envisageable et possible de changer de système après un délai donné et à des coûts acceptables (organisationnels, financiers, savoir-faire)
		Extraction des données	●	○		Les données propriétaires peuvent être extraites et/ou détruites lors d'un exit, suppression confirmable sur le plan organisationnel (selon possibilités légales)
Condition-cadre		Cadre juridique	●			Le cadre juridique du commanditaire est entièrement respecté
		Expertise	●			Le minimum de savoir-faire et de ressources pour gérer le système ou les partenaires sont disponibles en interne chez le commanditaire
		Contrats	●	○		Les contrats couvrent les exigences du système, de sa sécurité et sa souveraineté mais ne sont adaptables qu'à plus grands efforts pendant le cycle de vie du système

Tableau 3: Expression des différentes dimensions pour les variantes du type 1.

23 Les détails de toutes les variantes sont dans le document 3

24 Ceci pourrait être une acquisition par marché public de licences ou de la solution-même.

25 Le tableau ci-dessous représente, par dimension, les niveaux offerts comme valeur de base (●) dans ces variantes. Avec un effort supplémentaire (relativement) faible, il est possible d'atteindre un renforcement (○) de la souveraineté dans certaines dimensions.

5.3.2. *Types variantes 2 | Service Cloud « sur étagère » - configuré*

Variante 2a : Le métier achète un service standard avec certaines exigences de configuration dans les dimensions de souveraineté (lorsque c'est possible) pour la propre consommation ou l'IT l'achète pour le mettre à disposition du métier.

Exemple : Service suivi de tickets Jira acquis et exploité directement par un département métier interne. Configuré de façon à correspondre aux besoins et contrôles de souveraineté requis.

Variante 2b : L'IT engage un broker privé ou public pour mettre un service standard avec certaines exigences de configuration à disposition du métier et de l'IT.

Exemple : Service suivi de tickets Jira acquis et exploité par un prestataire de services IT du canton ou une entreprise privée spécialisée (broker). Configuré de façon à correspondre aux besoins et contrôles de souveraineté requis.

Variante 2c : Le métier achète un service standard avec des besoins prononcés sur le traitement et la localisation des données ou l'IT l'achète pour le mettre à disposition du métier.[26]

Exemple : Service suivi de tickets Jira exploité sur une infrastructure contrôlée par l'IT ou le broker, localisée en Suisse. Configuré de façon à correspondre aux besoins et contrôles de souveraineté requis.

L'objectif de ces variantes est de répondre à un cas d'usage en consommant un service standard d'un fournisseur de prestations *cloud* tout en imposant des restrictions dans les différentes dimensions de la souveraineté. Il s'agit en ce sens d'adapter l'utilisation et l'exploitation du système fourni aux exigences de souveraineté du commanditaire.

Le service peut être consommé directement chez le fournisseur, comme pour les variantes de type 1, nécessitant de manière additionnelle de la configuration afin de répondre aux exigences plus strictes (variantes 2a, 2c). Alternativement, le service avec des exigences de configuration peut être consommé à travers un broker (variante 2b). Les exigences de souveraineté se concentrent sur l'utilisation du service (focalisation : traitement et localisation des données, disponibilité, accès et gestion de l'évolution).

Comparaison par rapport aux variantes de type 1 :

Les variantes de type 2 sont similaires aux variantes de type 1, mais le commanditaire dispose d'un contrôle plus prononcé dans les dimensions de l'utilisation du système et surtout concernant le traitement et la localisation des données, grâce à la configuration. Ces variantes fournissent un niveau partiellement avancé d'exigences de souveraineté. La complexité de cette variante se trouve dans la contractualisation qui est plus poussée et dans l'utilisation du service qui nécessite plus d'efforts d'implémentation et d'exploitation. Dans le cas d'un service qui ne peut pas être configuré plus en profondeur, cette variante correspond à une variante 1.

[26] La variante 2c est un cas particulier de la variante 2a et est présentée ici séparément en raison de la priorité accordée à ces dimensions de localisation et traitement et stockage de données par les interlocuteurs des entretiens menés dans le cadre de cette étude.

Niveaux offerts par dimension des variantes de type 2

			Niveau 1	2	3	Exigences standard de souveraineté numérique
Cycle de vie	Création/ évolution	Développement du système	●	○		Pas de contrôle direct sur le développement et l'évolution, mais exigence de certifications et / ou audits correspondant(e)s
		Durabilité	●	○		Pas de contrôle direct sur la durabilité du système, mais exigence de certifications et / ou audits correspondant(e)s possibles
	Utilisation	Traitement des données	●	○		Les systèmes inclus dans la chaîne de traitement et de stockage ne sont pas strictement identifiés ou contrôlés
		Localisation des données		●		Les données sont traitées et stockées en Suisse, certaines (p. ex. données d'identité) en UE
		Disponibilité du système		●		La disponibilité du système est contrôlée par les choix architecturaux et est directement vérifiable de bout en bout par l'organisation
		Accès au système et aux données		●		Chaque accès est autorisé par le propriétaire des données et est vérifiable à tout moment, la chaîne de support est strictement contrôlée
		Gestion de l'évolution		●		Assurance que toute modification fonctionnelle ou financière du système ne sera mise en œuvre qu'après un délai convenu contractuellement
	Décommissionnement	Stratégie exit		●		Le système est concevable (p. ex. architecture, infrastructure) de façon à minimiser les coûts (organisationnels, financiers, savoir-faire) pour changer de système
		Extraction des données	●	○		Les données propriétaires peuvent être extraites et/ou détruites lors d'un exit, suppression confirmable sur le plan organisationnel (selon possibilités légales)
Condition-cadre		Cadre juridique	●	○		Le cadre juridique du commanditaire est entièrement respecté
		Expertise	●	○		Le minimum de savoir-faire et de ressources pour gérer le système ou les partenaires sont disponibles en interne chez le commanditaire
		Contrats	●	○		Les contrats couvrent les exigences du système, de sa sécurité et sa souveraineté mais ne sont adaptables qu'à plus grands efforts pendant le cycle de vie du système

Tableau 4: Expression des différentes dimensions pour les variantes du type 2.

5.3.3. Types variantes 3 | Service Cloud individualisé

Variante 3a : Le métier ou l'IT mandate et collabore avec un fournisseur pour développer un service individualisé.

Exemple : Plateforme reporting individualisée pour le métier ou l'IT du canton. L'individualisation de la plateforme la fait correspondre aux besoins et contrôles de souveraineté requis.

Variante 3b : Le mandat de développement et la mise à disposition du service au métier et à l'IT est gérée par un broker.

Exemple : Plateforme de reporting individualisée pour le métier ou l'IT du canton, exploitée par un prestataire de services IT du canton ou une entreprise privée spécialisée (broker). L'individualisation de la plateforme la fait correspondre aux besoins et contrôles de souveraineté requis.

L'objectif de ces variantes est de répondre à un cas d'usage en collaborant avec un fournisseur afin de créer ou adapter un service à des besoin individuels et d'obtenir ainsi un système pour lequel les exigences de souveraineté sont davantage définies. Cette variante met à la disposition du commanditaire des contrôles approfondis sur la **création**, **l'évolution**, **l'utilisation** et le **décommissionnement** du système ainsi que sur les **conditions-cadres**. Le commanditaire est alors en mesure de gestionner ou de surveiller toutes les dimensions du système tout en gardant la visibilité et en étant capable d'adapter la solution de manière plus flexible. Ces variantes fournissent un niveau avancé d'exigences de souveraineté.

Pour un cercle restreint d'utilisateurs, le développement du service peut être mandaté directement par l'administration cantonale (variante 3a), ou délégué à un broker (variante 3b) dans le cas où la complexité de la gestion est plus significative (complexité de la solution, nombre d'unités utilisant cette solution, nombre d'utilisateurs, etc.).

Comparaison par rapport aux variantes de type 2 :

Le service nécessaire pour les variantes de type 3 sort de l'offre standard des fournisseurs. Afin de consommer le service, un effort élevé est nécessaire en interne à l'administration pour mettre à disposition ce type de service : effort plus élevé pour la précision des exigences et des besoins, pour l'appel d'offre, pour la phase d'implémentation et l'exploitation en collaboration avec le fournisseur.

Niveaux offerts par dimension des variantes de type 3

			Niveau 1	Niveau 2	Niveau 3	Exigences standard de souveraineté numérique
Cycle de vie	Création/ évolution	Développement du système		●		Influence dans le développement et l'évolution, exigence de certifications et / ou audits correspondant(e)s possibles
		Durabilité		●		Influence sur la durabilité du système, exigence de certifications et / ou audits correspondant(e)s possibles
	Utilisation	Traitement des données		●	○	Les systèmes inclus dans la chaîne de traitement et de stockage sont connus ou contrôlés
		Localisation des données		●	○	Les données sont traitées et stockées en Suisse, sur des systèmes de stockage contrôlés par le commanditaire
		Disponibilité du système		●		La disponibilité du système est contrôlée par les choix architecturaux et est directement vérifiable de bout en bout par l'organisation
		Accès au système et aux données		●	○	Chaque accès est autorisé par le propriétaire des données grâce à des processus et systèmes sous contrôle du commanditaire
		Gestion de l'évolution		●		Assurance que toute modification fonctionnelle ou financière du système ne sera mise en œuvre qu'après un délai convenu contractuellement
	Décommissionnement	Stratégie exit		●		Le système est concevable (p. ex. architecture, infrastructure) de façon à minimiser les coûts (organisationnels, financiers, savoir-faire) pour changer de système
		Extraction des données		●		Les données propriétaires peuvent être facilement extraites et/ou détruites lors d'un exit, suppression prouvable sur le plan technique (selon possibilités légales)
Condition-cadre		Cadre juridique		●		Le cadre juridique est défini par le commanditaire (dans la mesure du possible) et est pleinement respecté
		Expertise	●	○		Le minimum de savoir-faire et de ressources pour gérer le système ou les partenaires sont disponibles en interne chez le commanditaire
		Contrats		●		Les contrats couvrent les exigences du système, de sa sécurité et sa souveraineté et peuvent être adaptés selon l'évolution des besoins après un délai prédéfini

Tableau 5: Expression des différentes dimensions pour les variantes du type 3.

5.3.4. *Types variantes 4 | Service Cloud en développement propre*

Variante 4a : Développement d'un service individuellement par une entité représentant une administration cantonale.

Exemple : Système de stockage de données Dell, développé spécifiquement pour le métier ou l'IT du canton. Le système est sous contrôle total du commanditaire et l'expertise interne est suffisante pour l'exploitation et l'évolution du système.

Variante 4b : Développement d'un service propre à une entité publique qui met à disposition le service pour une communauté indépendante.

Exemple : Système de stockage de données Dell, développé et exploité spécifiquement pour les métiers ou les IT des cantons par un prestataire de services IT d'une entité publique[27] ou privée spécialisée (broker). Le système est sous contrôle total.

L'objectif de ces variantes est de répondre à un cas d'usage en développant soi-même ou sur mandat un service cloud et de fournir un contrôle total. Ceci afin que le commanditaire puisse maîtriser complètement ses systèmes. Celui-ci peut gérer entièrement les applications, les plateformes et les infrastructures, entre autres, qui sont sous-jacentes aux solutions choisies. Ces variantes garantissent un niveau supérieur d'exigences de souveraineté.

Le développement du service peut être fait et consommé directement par l'administration cantonale, respectivement par une entité qui la représente (variante 4a). En cas de besoins inter-organisationnels, un broker public peut développer un service propre à une communauté (variante 4b).

Comparaison par rapport aux variantes de type 3 :

Pour les variantes de type 4, l'administration cantonale possède totalement le service. Les fournisseurs de service, qui répondraient aux exigences des variantes de type 3, peuvent fournir des services pour les variantes de type 4, mais uniquement sous la gestion totale du comandataire. La complexité additionnelle reflète la prise en charge complète du service par l'administration cantonale, car elle prend la responsabilité de tous les rôles auparavant repartis entre plusieurs entités. L'effort nécessaire pour le développement, l'exploitation et le décommissionnement est plus élevé. Certaines tâches peuvent être délégués avec des contrats respectifs, mais la coordination et l'harmonisation en service cohérent reste dans la responsabilité de l'administration cantonale.

[27] Aujourd'hui, il n'y a pas encore d'entité publique qui pourrait jouer le rôle de broker pour une administration cantonale. L'initialisation de cette entité nécessiterait un montant considérable à court terme, afin de garantir une offre similaire à un broker privé (pour autant que ce soit souhaitable). Les désavantages de la dépendance et des conflits d'intérêts potentiels, qui sont directement liés à la souveraineté, pourraient être réduits avec un broker public. Des exemples pourraient être un canton lui-même, eOperations Schweiz, l'OFIT ou l'ANS (le délégant à une autre entité).

Niveaux offerts par dimension des variantes de type 4

			Niveau 1	2	3	Exigences standard de souveraineté numérique
Cycle de vie	Création/ évolution	Développement du système			•	Contrôle direct sur le développement et l'évolution du système
		Durabilité			•	Contrôle direct sur la durabilité du système
	Utilisation	Traitement des données			•	Les systèmes inclus dans la chaîne de traitement et de stockage sont sous le contrôle du commanditaire
		Localisation des données			•	Les données sont traitées et stockées en Suisse, sur des systèmes de stockage contrôlés par le commanditaire
		Disponibilité du système			•	Tous les systèmes, et donc aussi leurs disponibilités, sont sous contrôle du commanditaire
		Accès au système et aux données			•	Chaque accès est autorisé par le propriétaire des données grâce à des processus et systèmes sous contrôle du commanditaire
		Gestion de l'évolution			•	Toute modification fonctionnelle ou financière du système est contrôlée par le commanditaire (au maximum techniquement possible)
	Décommissionnement	Stratégie exit			•	Le système est conçu (p. ex. architecture, infrastructure) par le commanditaire et le changement de système est contrôlé par le même
		Extraction des données			•	Le système est contrôlé par le commanditaire et l'extraction et/ou la destruction des données propriétaires aussi (selon possibilités légales)
Condition-cadre		Cadre juridique			•	Le cadre juridique ne concerne que le commanditaire ou est défini par lui de manière significative (dans la mesure du possible) et est entièrement respecté
		Expertise			•	Le cycle de vie du système repose en grande partie sur le savoir-faire et les ressources du commanditaire
		Contrats			•	Le fournisseur agit pour le compte et dans l'intérêt direct du commanditaire, les contrats (si existants) sont facilement adaptables

Tableau 6: Expression des différentes dimensions pour les variantes du type 4.

5.4. Évaluation des variantes

Toutes les variantes présentées ci-dessus remplissent les exigences de souveraineté à un certain degré. Le présent chapitre met en perspective la souveraineté avec la complexité, les coûts et la sécurité des variantes présentées.

5.4.1. Évaluation des variantes en termes de complexité et coûts vs. souveraineté

Le graphique suivant présente la relation entre la souveraineté atteinte et la complexité liée à chacune des variantes. La complexité est ici une mesure qui résume la complexité de mise en œuvre d'un système, son acquisition et son exploitation jusqu'à son décommissionnement. La taille des bulles est proportionnelle aux coûts (relatifs) de chaque variante.

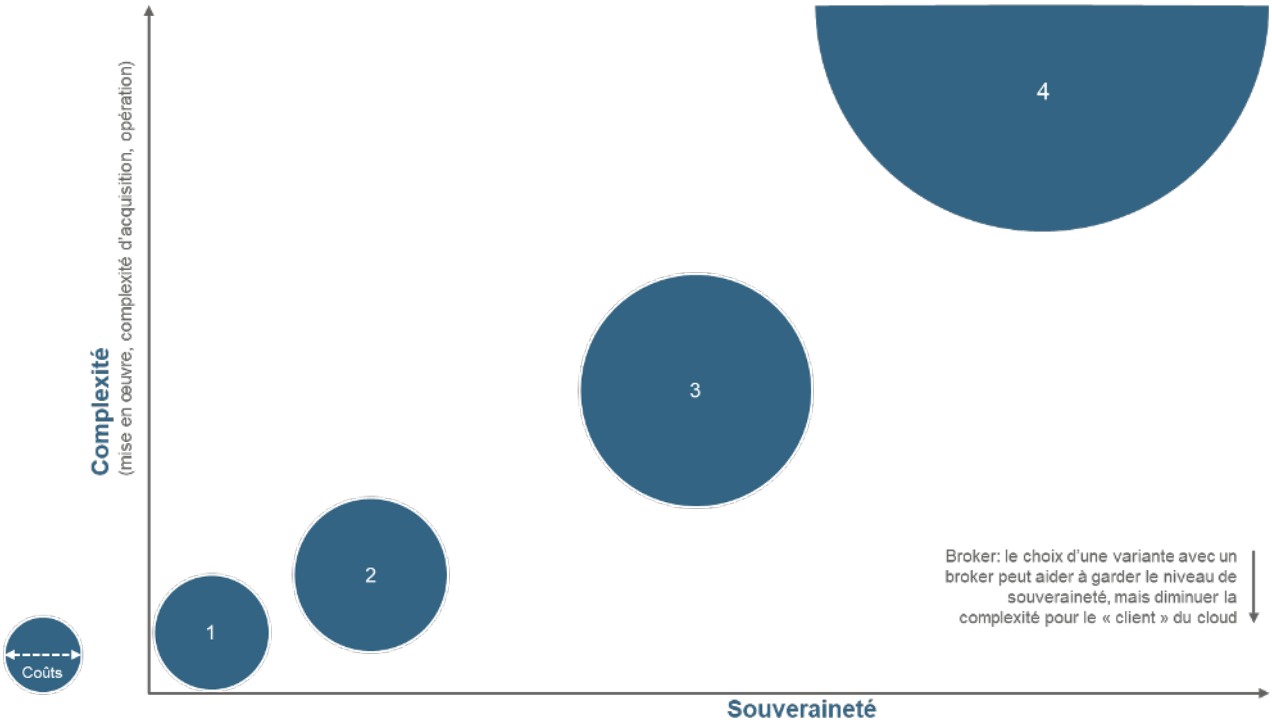

Figure 7: Relation entre la souveraineté et la complexité des variantes. Ce graphique sert uniquement à indiquer des ordres de grandeur et ne représente pas des valeurs clairement mesurables.

De manière générale, l'indication est que (a) les exigences en matière de souveraineté ont un impact sur les dépenses nécessaires à la mise en place des systèmes correspondants (un contrôle et une autonomie accrus nécessitent les connaissances, l'organisation et les processus nécessaires ainsi que les ressources techniques et humaines requises) et (b) les différentes dimensions de la souveraineté ne peuvent souvent pas être dissociées les unes des autres – une souveraineté accrue dans une dimension peut également entraîner la complexité d'autres dimensions.

5.4.2. *Évaluation des variantes en termes de sécurité vs. souveraineté*

Le graphique ci-dessous présente la relation entre la souveraineté choisie et la contribution personnelle à la cybersécurité dans le cadre des variantes. Il montre, comme le graphique précédent, que la responsabilité organisationnelle en matière de cybersécurité augmente avec la souveraineté.

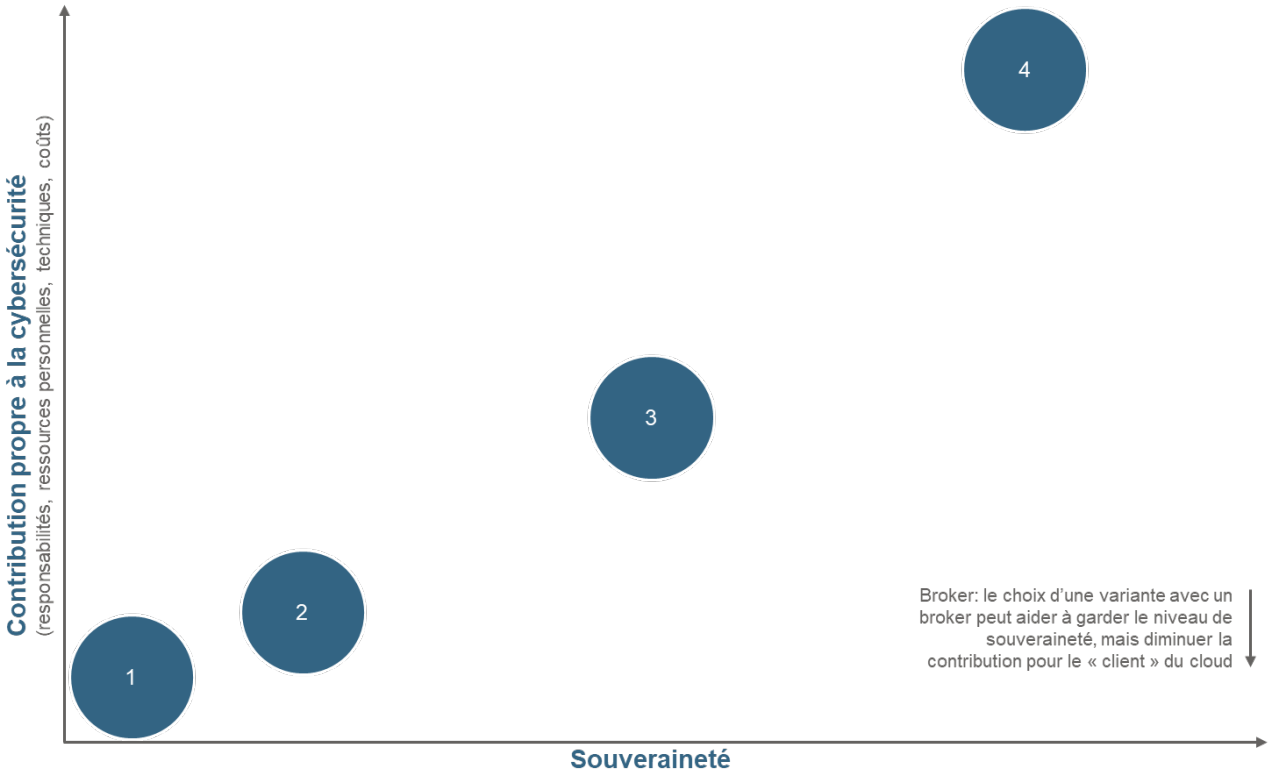

Figure 8: Relation entre la souveraineté et les coûts d'investissement pour garantir la sécurité. Ce graphique sert uniquement à indiquer des ordres de grandeur et ne représente pas des valeurs clairement mesurables. La sécurité est un aspect pertinent de la souveraineté, mais la souveraineté couvre également d'autres thèmes de même importance.

La sécurité perçue est (comme dans l'environnement privé) fortement marquée par le contrôle personnel, même si cela peut être trompeur dans de nombreux cas : il convient de noter que les entreprises spécialisées (fournisseurs de services cloud et notamment *hyperscaler*) ont une très grande expérience et les ressources[28] correspondantes pour mettre en place, maintenir et renforcer en permanence la cybersécurité des systèmes.

D'un point de vue de la sécurité, les services offerts par des fournisseurs établis dans le marché, c'est-à-dire les variantes de type 1 et 2, respectent des standards très élevés. Ces fournisseurs ont la possibilité d'investir des ressources importantes dans le développement de leurs systèmes pour la protection contre les risques liés à la cybersécurité. Plus les variantes ont une souveraineté élevée, plus les solutions s'éloignent du standard et avec ça l'effort pour garantir la sécurité est élevé.

Il faut également noter que la localisation des systèmes dans un espace juridique donné (p. ex. la Suisse) n'augmente la cybersécurité que sur une base juridique, et non pas sur une base technique.

[28] Exemple : Investissements Microsoft, Google : Lien

5.4.3. Évaluation des variantes en termes de cas d'usage

Toutes les variantes décrites ci-dessus sont réalisables d'un point de vue technique et organisationnel, mais ne sont pas forcément toutes appropriées à chaque cas d'usage pour une administration cantonale : certains systèmes n'offrent pas suffisamment de possibilités de configuration/contrôle pour être construits dans la variante souhaitée. Par exemple, il serait techniquement possible, mais irréaliste, de construire soi-même des systèmes comme deepl.com ou des composants hardware.

Chaque administration cantonale qui envisage d'appliquer les dimensions élaborées dans cette étude doit individuellement évaluer chacune des variantes pour ses cas d'usage.

Le tableau ci-dessous propose des exemples de systèmes et une première réflexion sur les variantes qui leur correspondaient.

Sytème / Variante	Service Cloud « Sur étagère »		Service Cloud « Sur étagère » - configuré			Service Cloud Individualisé		Service Cloud Développement propre	
	Var. 1a	Var. 1b	Var. 2a	Var. 2b	Var. 2c	Var. 3a	Var. 3b	Var. 4a	Var. 4b
SaaS à configuration limitée, p. ex. Miro	x	x							
SaaS configurable, p. ex. Salesforce	x	x	x	x	x				
Containerisation sur Cloud (PaaS)	x	x	x	x	x	x	x		x
Application métier, données publiques, besoins individuels						x	x	x	x
VMs (IaaS)	x	x	x	x	x	x	x		x
Hardware	x	x							
M365 / G Workspace / Suite éditage de documents	x	x		x					
Traitement et stockage de données publiques	x	x	x	x	x	x	x		x
Traitement et stockage de données internes			x	x	x	x	x	x	x
Traitement et stockage de données confidentielles						x	x	x	x
Traitement et stockage de données secrètes								x	x

Tableau 9: Exemples de systèmes et variantes possibles correspondantes

Le choix de variantes idéal pour des cas d'usage comme des applications métier, solutions de monitoring / logging ou stockage de clés d'accès dépend toujours des données traitées et stockées par celles-ci. Le tableau ci-dessus présente une base de réflexion à ce sujet et n'est donc pas une proposition.

5.5. Modèle pour identifier la variante optimale sur la base d'un cas d'usage

Sur la base des points de discussion mentionnés ci-dessus, ce chapitre présente une procédure qui peut être utilisée par une administration cantonale pour sélectionner une variante de mise en œuvre pour un cas d'usage et un système donné. Il convient de noter que la mise en œuvre peut inclure différentes variantes – les différents sous-systèmes peuvent tous être implémentés par une variante différente. Il faut donc toujours considérer l'ensemble de la « chaîne d'approvisionnement » d'un système et l'optimiser au niveau local ou global.

Le modèle expliqué ici est structuré dans les différentes étapes à élaborer par l'administration publique et un exemple simple pour un cas d'usage d'un service web classique est présenté dans l'annexe A.4. La procédure est la suivante :

1. Définition du cas d'usage, identification des systèmes impliqués et des conditions-cadres (cadre juridique, expertise, contrats)
2. Classification des données, afin d'identifier les exigences spécifiques des données traitées dans ce cas d'usage
3. Décomposition de la solution en sous-systèmes, afin d'identifier les exigences spécifiques plus nuancées
4. Évaluation des exigences en matière de souveraineté pour chacun des sous-systèmes
5. Attribution des variantes pour chacun des sous-systèmes et optimisation
6. Mise en œuvre de la variante avec un achat, resp. un développement

Cette procédure ne peut pas faire l'économie d'une réflexion globale, dans laquelle s'inscrit une vision d'ensemble de tous les cas d'usage. De plus, cette réflexion globale doit permettre d'inscrire l'utilisation des technologies cloud dans l'action et la vision globale de l'Etat en matière de transition numérique.

6. Conclusion et recommandations

Dans cette étude la notion de souveraineté numérique a été définie et appliquée aux technologies cloud afin de définir la notion d'un *cloud* souverain. Il en résulte que la souveraineté numérique se compose de différentes dimensions. Un niveau de souveraineté (1 = peu souverain à 3 = très souverain) peut être attribué à chacune des dimensions. Il n'y a donc pas un seul niveau de souveraineté absolu qui caractérise un *cloud* souverain en général, ni dans chacune des dimensions. Pour appliquer les dimensions de la souveraineté numérique développées dans le cadre de la présente étude à un cas d'usage, il est nécessaire d'identifier en premier lieu les aspects organisationnels et techniques qui doivent atteindre un certain degré de souveraineté et de les mettre en relation avec les dimensions de la souveraineté numérique.

Toutes les variantes présentées dans cette étude sont des variantes d'opportunité de « *cloud* souverain » pour différents degrés de souveraineté requis. L'analyse qui est basée sur l'hypothèse qu'un *cloud* souverain est nécessaire, démontre qu'il n'existe pas de solution unique pour un *cloud* souverain. La Figure 1 démontre que les coûts augmentent drastiquement pour une souveraineté élevée. Donc il est nécessaire que chaque administration publique identifie au cas par cas quels sont ses besoins et quelle variante y répond le mieux.

Pour conclure, l'étude n'a ni identifié ni considéré l'opportunité d'un unique *cloud* souverain commun entre les cantons latins. Les recommandations qui suivent sont formulées par le mandataire. Elles visent à initier des démarches au sein des différents cantons, afin d'élaborer des plans d'actions qui pourraient déboucher sur des mutualisations. Ces derniers devraient considérer les exigences envers la souveraineté, l'identification des cas d'usage et la classification des données ainsi que la recherche de synergies possibles au sein de l'écosystème des administrations cantonales.

En ce sens, la présente étude offre un cadre de référence pour accompagner les cantons dans leurs démarches respectives.

6.1. Recommandations

Sur la base des résultats de cette étude, les auteurs de la présente étude émettent les recommandations suivantes pour améliorer l'utilisation du *cloud* souverain dans le secteur public et parapublic :

6.1.1. Élaboration des principes et stratégies pour l'utilisation de service cloud pour les administrations cantonales

Il est recommandé d'élaborer des principes pour l'utilisation de services cloud pour les administrations cantonales et les institutions parapubliques permettant d'orienter les acteurs dans le développement de leurs stratégies *cloud*. Ainsi, il est recommandé que chaque canton élabore une stratégie *cloud* pour les trois à cinq prochaines années sur cette base, afin d'adresser les enjeux évoqués dans cette étude.

La stratégie doit permettre d'une part de guider les administrations dans l'utilisation des services cloud en général mais surtout pour les services souverains, afin de profiter de ce levier de l'innovation, et d'autre part d'initier une adaptation des bases légales et des procédures administratives, lorsque c'est nécessaire. Il est recommandé d'orienter l'aspect de souveraineté dans les stratégies *cloud* envers une approche couvrant une multitude des variantes mentionnées dans cette étude. Cette stratégie doit également préparer le cadre pour les nouveaux rôles qui vont gagner en importance au sein des organisations IT et les processus de financement qui nécessiteront des adaptations au sein des administrations publiques.

6.1.2. *Identifier les cas d'usage pour l'utilisation de services cloud et effectuer une classification détaillée des données*

Il est recommandé que les administrations cantonales identifient leurs cas d'usage pour des services cloud. Afin de pouvoir caractériser proprement le cas d'usage, il est nécessaire de comprendre en détail les processus, les systèmes concernés et les données qui y sont traitées. Il est donc recommandé que chaque administration classifie[29] systématiquement ses données à travers tous les processus métiers. Cette classification permettrait de définir les exigences envers la souveraineté et d'évaluer plus simplement les cas d'usage (et les cas d'usage futurs). La grille de classification pourrait faire l'objet d'un consensus entre les cantons. Les douze dimensions identifiées dans cette étude peuvent être utilisées comme guide pour trouver une variante répondant à toutes les exigences de souveraineté propres à chaque cas d'usage.

6.1.3. *Identifier les synergies et les opportunités pour l'utilisation de services cloud pour toutes les administrations cantonales par un broker*

Sur la base des résultats des recommandations précédentes et des exigences qui en résultent, ainsi que sur le fait que des variantes avec le plus haut degré de souveraineté ont des coûts importants, il est recommandé d'identifier les synergies possibles résultant de solutions intercantonales. Pour cela, il est recommandé d'impliquer toutes les organisations qui ont un intérêt – les administrations cantonales de divers cantons, des administrations communales, des organisations parapubliques et de l'Administration Numérique Suisse.

Ainsi, il est recommandé d'identifier et d'analyser les synergies pour l'utilisation de services cloud à travers un broker public ou privé, pour les acteurs du secteur public. Pour cela il faut identifier les différentes entités publiques ou privées qui pourraient assumer ce rôle de broker. Aujourd'hui, il n'y a pas encore d'entité publique qui pourrait jouer ce rôle. L'initialisation de cette entité nécessiterait un montant considérable à court terme, afin de garantir une offre similaire à un broker privé. Un broker public pourrait néanmoins réduire la dépendance et les conflits d'intérêts potentiels (et ainsi augmenter la souveraineté). Des exemples d'entités à analyser qui pourraient prendre le rôle de broker seraient eOperations Schweiz, l'OFIT ou l'ANS (le délégant à une autre entité) ou un canton lui-même.

6.1.4. *Créer un référentiel pour guider les démarches communes liées à la souveraineté dans le cloud*

Afin de garantir une compréhension de la souveraineté appliquée au *cloud* commune à toutes les administrations cantonales, il est recommandé de formaliser cette définition sous forme de référentiel, de manière similaire aux référentiels pour la sécurité dans le *cloud* (c.f. 0).

Ce référentiel pourrait être constitué de la définition de la souveraineté numérique et de son application aux services cloud ainsi que d'exigences de souveraineté spécifiques à des cas d'usage. Il pourrait également nourrir les discussions dans la recommandation précédente. Ces exigences peuvent être utilisées pour créer des offres « souveraines ». Dans le cadre de l'élaboration de ce référentiel, il est recommandé d'analyser les possibilités d'utiliser une entité publique ou privée évaluant et labellisant des services cloud spécifiques sur la base de ce référentiel.

Après avoir gagné en maturité avec un référentiel, une ou plusieurs normes dominantes dans la thématique de la souveraineté numérique dans le *cloud* peuvent en résulter et ces normes peuvent être utilisées pour des certifications.

[29] La classification des données est le processus par lequel les données structurées ou non structurées sont analysées et classées dans des catégories définies en fonction du type de fichier et de son contenu.

6.1.5. Hors-périmètre – Prévoir une infrastructure numérique souveraine pour le contexte géopolitique de « crise »

Aujourd'hui, il n'y a pas de solution pour un *cloud* souverain, ni d'infrastructure au sens large dans un contexte géopolitique de « crise » pour les administration cantonales (voir 4.2.2) et le passage d'un contexte stable à un contexte de crise doit être minutieusement préparé. Ce passage nécessite différents plans, notamment un plan de reprise après sinistre (desaster recovery plan) et un plan pour la migration vers les systèmes hautement souverains. Ce concept se base sur les résultats des recommandations précédentes, car seulement les services les plus fondamentaux et avec les exigences envers la souveraineté les plus élevées seront pertinents pour ce *cloud* souverain en contexte de « crise ». Envisageant des coûts considérables pour la réalisation de cette infrastructure, une collaboration intercantonale est indispensable.

6.1.6. Hors-périmètre – Initiative Gaia-X

Dans le cadre de cette étude il n'y a pas de recommandation concernant l'initiative Gaia-X. Le Conseil fédéral a initié une analyse à la participation au projet Gaia-X qui sera entre autres menée par l'ANS. Le projet Gaia-X couvre plusieurs des dimensions de la souveraineté défini dans cette étude, mais a comme objectif de favoriser l'adoption du *cloud computing*, d'accélérer l'économie de la donnée et de construire les briques technologiques nécessaires à la circulation de la donnée en Europe.

A. Annexes

A.1. Définition « cloud »

Le terme « cloud » est utilisé dans des contextes très différents et est parfois devenu un terme marketing utilisé par différents fournisseurs de solutions informatiques et d'autres produits. Dans le cadre des entretiens faits durant cette étude il a été constaté qu'il y a différentes compréhensions des termes « cloud », « service cloud » et « souveraineté ».

Pour parvenir à un consensus et afin d'avoir une compréhension commune entre les différentes parties prenantes, la définition la plus courante du cloud et de ses caractéristiques a été utilisée. Elle se base sur le modèle NIST [30]:

- **Libre-service à la demande :** le provisionnement des ressources (p. ex. puissance de calcul, stockage) s'effectue de manière automatisée sans interaction avec le fournisseur de services.
- **Large accès au réseau :** les services sont disponibles via le réseau grâce à des mécanismes standard et ne sont pas liés à un client/terminal particulier.
- **Regroupement des ressources :** les ressources du fournisseur de services sont disponibles dans un pool dans lequel de nombreux utilisateurs peuvent se servir (modèle multi tenant), les utilisateurs ne sachant pas nécessairement où se trouvent les ressources.
- **Disponibilité rapide et flexible :** les services peuvent être mis à disposition rapidement et de manière flexible, dans certains cas même de manière automatisée. Du point de vue de l'utilisateur, les ressources semblent donc infinies.
- **Mesure de l'utilisation :** l'utilisation des ressources peut être mesurée (p. ex. pour la facturation) et surveillée, et peut également être mise à la disposition des utilisateurs.

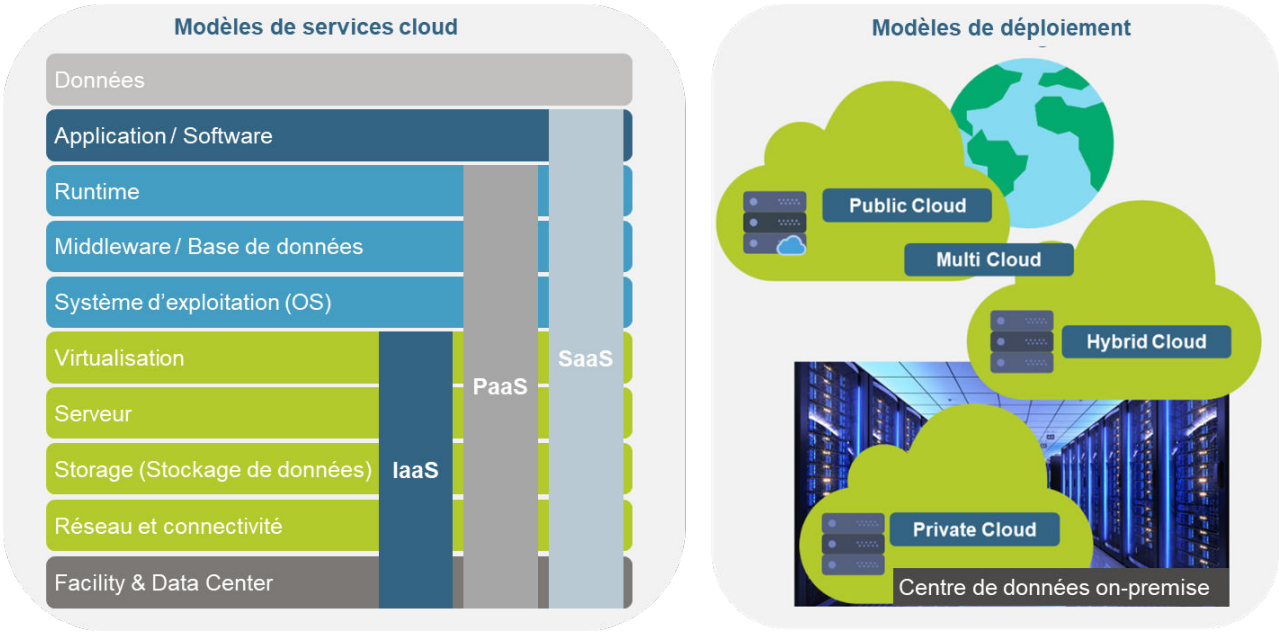

Figure 10: Modèles de services en cloud et modèles de déploiement

[30] https://www.nist.gov/

Modèles de services cloud	Description
SaaS (Software-as-a-Service)	Solution logicielle ou programmes d'application entièrement mis à disposition par le fournisseur de cloud et accessibles aux utilisateurs via un navigateur web sur le réseau.
PaaS (Platform-as-a-Service)	Les utilisateurs installent, gèrent et exploitent aussi bien leurs propres développements que des applications tierces avec les langages de programmation et les environnements d'exécution pris en charge par le fournisseur de cloud.
IaaS (Infrastructure-as-a-Service)	Les utilisateurs ne sont pas responsables de la gestion des ressources physiques et virtuelles sous-jacentes, mais gèrent le système d'exploitation, le stockage des données et mettent à disposition les applications qui utilisent les ressources sous-jacentes.

Modèles de déploiement cloud	Description
Public Cloud	Ressources cloud multi-tenant, accessibles au public, avec une évolutivité pratiquement "illimitée".
Private Cloud	Environnement cloud exploité exclusivement pour une seule organisation
Hybrid Cloud	Utilisation simultanée de services de cloud public et privé ou de déploiements *on-premise* au sein de la même architecture système
Multi Cloud	Utilisation simultanée des services cloud de différents fournisseurs cloud, utilisés simultanément dans une architecture système hétérogène.
Community Cloud	Cas particulier du cloud privé, qui est exploité de manière dédiée pour un groupe d'organisations ayant des intérêts similaires

A.2. Listes des parties prenantes consultées lors de l'élaboration de l'étude

Afin de récolter et de comprendre les besoins actuels des administrations cantonales pour les services cloud ainsi qu'envers la souveraineté, tous les Cantons latins ont été consultés par le biais d'interviews. Tous les entretiens ont été effectués à l'aide de guides d'entretiens structurés afin de garantir la comparabilité des résultats. Les questions posées visent à explorer les aspects stratégiques, métiers et techniques.

Le tableau suivant présente la liste des personnes et organisations interviewées dans le cadre de l'étude.

Nom	Organisation	Rôle
Amintore Savini	Canton de Vaud, DGNSI	Directeur PS-MET
Hervé de Nicola	Canton de Vaud, DGNSI	Directeur PS-TEC
Pascal Hallard	Canton de Vaud, DGNSI	Architecte d'entreprise
Eric Favre	Canton de Genève, OCSIN	Directeur général OCSIN
Olivier Baujard	Canton de Genève, OCSIN	Chef de service
Christophe Mistral	Canton de Genève, OCSIN	Conseiller de direction
Tom Royston	Ville de Genève, DSIC	Directeur DSIC
Sébastien Chèvre	Canton de Jura	Architecte d'entreprise
Daniel Crevoisier	Canton de Neuchâtel	Chef de service
Silvano Petrini	Canton du Tessin	Direttore
Bertrand Zermatten	Canton du Valais	Architecte d'entreprise
Michel Demierre	Canton de Fribourg	Head of IT and Telecommunications
Jean-Francois Pradeau	Hôpitaux universitaires de Genève	Directeur Direction des Systèmes d'Information
Thomas Jacobsen	Infomaniak	Communication Manager
Lukas Greve	Infomaniak	Pre-Sales Engineer
Christophe Gerber	Elca	General Manager
Severin Voisin	Elca	Directeur Elca Cloud
Yves Pitton	Elca	Direction Swiss Business Solutions
Christian Widmer	Microsoft	Director Public Sector
Marc Holitscher	Microsoft	National Technology Officer
Marc Meigner	Oracle	Senior Director, Dedicated Region Cloud@Customer lead
Nathalie Sers	Oracle	Senior Cloud Sales Representative
Marc Wittmer	Exoscale	Sales Specialist Cloud

A.3. Abréviations et termes

Abréviation	Description
ANS	Administration numérique suisse
BCR	Binding Corporate Rules
BMWi	Bundesministerium für Wirtschaft und Energie (nouveau nom: Bundesministerium für Wirtschaft und Klimaschutz (BMWK)
CJUE	Cours de justice de l'union européenne
CLDN	Conférence latine des directeurs du numérique
CP	Code pénal
DGNSI	Direction générale du numérique et des systèmes du canton de Vaud
DSIC	Direction des systèmes d'information et de communication du canton de Genève
EPFL	École polytechnique fédérale de Lausanne
IaaS	Infrastructure as a Service
IoT	Internet of Things
LPD	Loi fédérale sur la protection des données
LPrD	Loi sur la protection des données personnelles
NIST	National Institute of Standards and Technology
nLPD	Nouvelle loi sur la protection des données
OCSIN	Office cantonale des systèmes d'information et du numérique
PaaS	Platform as a Service
PFPDT	Préposé fédéral à la protection des données et à la transparence
RGPD	Règlement général de l'UE sur la protection des données
SaaS	Software as a Service
SCC	Standard Contractual Clauses
UE	Union Européenne
VM	Virtual Machine

A.4. Exemple d'application du modèle

Le modèle expliqué dans le chapitre 5.5 est illustré ici avec un exemple simple et concret : un service web pour un service pour un citoyen (p. ex. une demande de permis de construction). La spécificité de cet exemple est que les données saisies ne sont pas critiques, mais que la consolidation et l'analyse des données long terme le sont.

1. Définition du cas d'usage, identification des systèmes impliqués et des conditions-cadres (cadre juridique, expertise, contrats)

Le cas d'usage et les conditions cadres sont identifiés. Le service web possède des informations publiques, offre des formulaires pour des particuliers, analyse des données et stocke les résultats à long terme. Le système est donc composé d'un front-end, d'un back-end spécialisé, d'une base de données, d'une logique analytique et d'une base de données pour les données long terme.

2. Classification des données, afin d'identifier les exigences spécifiques des données traitées dans ce cas d'usage

Les données sont classifiées selon les directives en vigueur.

3. Décomposition de la solution en sous-systèmes, afin d'identifier les exigences spécifiques plus nuancées

La décomposition de la solution en ses sous-systèmes aide à considérer les exigences de manière plus nuancée, car chacun a un périmètre plus spécifique et des exigences plus clairement différenciées quant à son cycle de vie et au contrôle nécessaire.

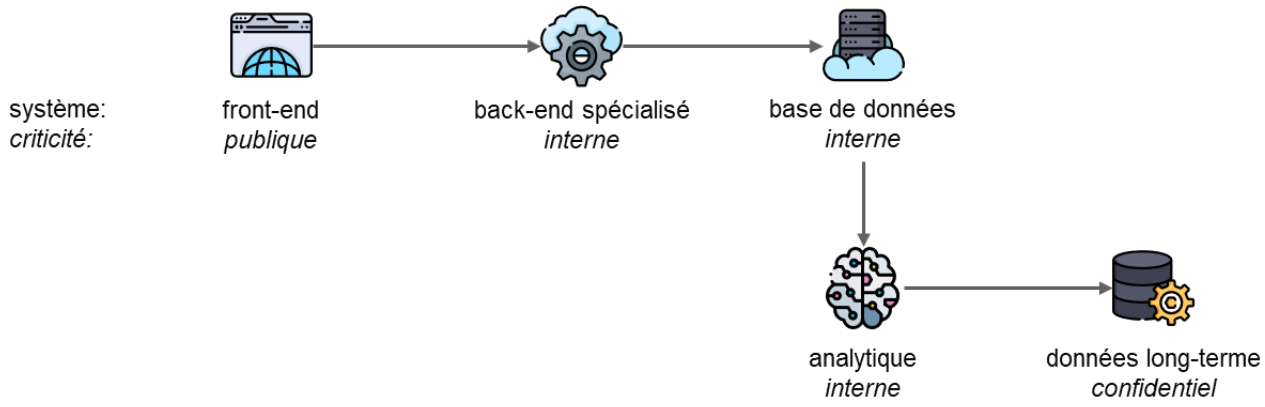

Figure 11:Exemple de solution – vue sous-systèmes

4. Évaluation des exigences en matière de souveraineté pour chacun des sous-systèmes

Après une première description rudimentaire de l'architecture de la solution globale et de ses sous-systèmes, il est possible, dans une étape suivante, de procéder à un relevé des exigences en matière de souveraineté. Le choix des variantes peut maintenant être fait au niveau des sous-systèmes, sur la base des exigences (choisies ici dans cet exemple de manière à peu près arbitraire) relatives aux dimensions de la souveraineté.

			Exigences par sous-système (niveau)				
			front-end	back-end spécialisé	base de données	analytique	données long-terme
Cycle de vie	Création/ évolution	Développement du système	1	2	1	1	1
		Durabilité	1	2	1	1	1
	Utilisation	Traitement des données	1	1	2	2	3
		Localisation des données	1	1	2	2	3
		Disponibilité du système	2	2	2	1	2
		Accès au système et aux données	2	2	2	2	3
		Gestion de l'évolution	1	2	1	1	1
	Décommissionnement	Stratégie exit	1	2	1	1	3
		Extraction des données	1	2	2	1	3
Condition cadre		Cadre juridique	1	2	2	2	3
		Expertise	1	2	1	1	2
		Contrats	1	2	2	2	3
Variante choisie			Type 1	Type 3	Type 2	Type 2	Type 4

Figure 12: Exemple de solution – évaluation des exigences dans les niveaux (1-3) de souveraineté comme décrit dans le chapitre 4.3.1

5. Attribution des variantes pour chacun des sous-systèmes et optimisation

Le choix de la variante d'un point de vue de souveraineté pour le sous-système résulte donc des exigences envers chaque dimension. Les exigences peuvent être mises en relation avec le niveau de souveraineté atteint par type de variante (c.f. Tableau 3, Tableau 4, Tableau 5, Tableau 6). Lors du choix effectif des types de variantes, il est bien sûr possible, selon les besoins, de n'évaluer qu'une partie des dimensions comme pertinentes ou importantes (pondération), ce qui permet d'affiner le choix.

Le back-end spécialisé existe éventuellement déjà sur un environnement correspondant à une variante 3. C'est pourquoi un tel environnement a été choisi au lieu d'une variante 2. Sur la base de l'expertise existante et des contrats ou partenariats existants, une variante spécifique peut également être choisie. Cela donnerait la situation intermédiaire suivante.

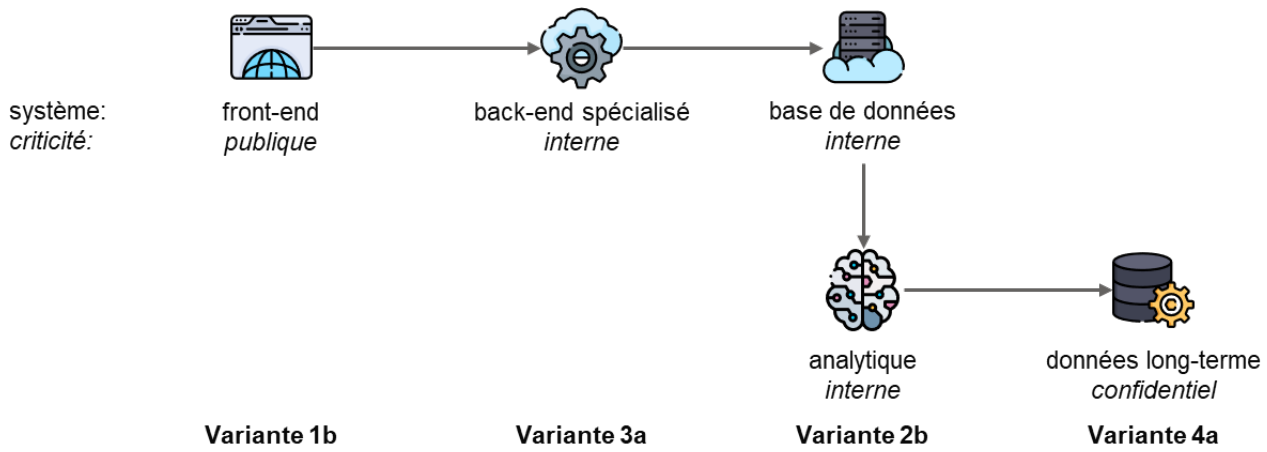

Figure 13: Exemple de solution – vue sous-systèmes avec variantes choisies

Dans une itération complémentaire, le choix peut être optimisé (minimiser le nombre de plateformes différentes, minimiser la complexité de la mise en place du système et de son fonctionnement durable) afin de minimiser le nombre de solutions séparées. Il est important de ne pas descendre en dessous des exigences posées en matière de souveraineté – il ne faudrait donc choisir qu'une variante qui soit « plus forte ». Une solution viable serait donc de réduire le choix à une Variante 2b (front-end, base de données et analytique) et une Variante 4a (back-end spécialisé et données long-terme) qui pourraient suffire pour exploiter cette solution.

Il serait bien évidement possible de choisir, sur la base des exigences de criticité données, une variante de type 4 qui couvre toutes les exigences relatives aux dimensions de la souveraineté. Cependant, cela ne tiendrait pas compte du fait que des optimisations de la complexité de la mise en place du système et de son fonctionnement durable seraient éventuellement possibles.

6. Mise en œuvre de la variante avec un achat, resp. un développement

Une fois les variantes choisies, une analyse des besoins et des ressources disponibles peut être effectuée (y compris des fournisseurs / partenariats existants et des ressources techniques et personnelles internes). Celles-ci peuvent ensuite être évaluées les unes par rapport aux autres (sur la base des autres exigences existantes) afin d'aboutir à un choix. Si nécessaire, un appel d'offres doit être réalisé.