Droit et technique II

Master 1ère année

Cloud computing et protection des données

Mémoire présenté par

ALEXIS DE ARAGAO

ETUDIANT EPFL

Mémoire dirigé par

MAXIMILIEN STAUBER

CHARGE DE COURS SHS/UNIL

ALEXANDRE CHABENET

ASSISTANT SHS/ UNIL

Année 2022/2023

Table des matières

Introduction **2**

1. Définition du cloud computing **2**

2. Régime juridique suisse en matière de protection des données et cloud computing **4**

3. Protection des données des personnes physiques (nLPD) et cloud computing **5**

3.1. Champ d'application matériel, personnel et territorial de la nLPD (art. 2, 3 et 5, nLPD) 5

3.2. Principes érigés dans la nLPD (art. 6, nLPD), à respecter lors du traitement dans le cloud ... 6

3.3. Mesures organisationnelles et techniques à observer par le responsable du traitement de données et le prestataire cloud (art. 7 et 8, nLPD, et art. 3, nOPDo) 11

3.4. Conditions à la sous-traitance du traitement de données dans le cloud (art. 9, nLPD) 13

3.5. Conditions à satisfaire lors de la communication transfrontalière de données vers le cloud (art. 16ss, nLPD) 15

3.6. Devoir du responsable du traitement d'informer la personne dont les données sont traitées dans le cloud (art. 19ss, nLPD) 17

3.7. Droits de la personne concernée (art. 25ss, nLPD) 18

4. Casus : le projet de cloud computing "Public Clouds Confederation" est-t-il compatible avec le droit suisse en matière de protection des données pour les personnes physiques ? .. 21

4.1. Historique du projet "Public Clouds Confederation" 21

4.2. Conformité du projet "Public Clouds Confederation" avec la nLPD 23

Bibliographie **25**

Glossaire des acronymes
(non-définis dans le mémoire)

VPN: acronyme pour Virtual private network, réseau privé virtuel en français. Système créant une connexion privée entre des ordinateurs distants et permettant un échange de données sans recourir à un réseau public de télécommunication (comme Internet).
Secteur TNI: acronyme pour l'unité "Transformation numérique et gouvernance de l'informatique" de la Chancellerie fédérale, chargée d'encourager et de coordonner la transformation numérique de l'administration fédérale depuis le 1er janvier 2021.
TAF: tribunal administratif fédéral. Instance de recours contre les décisions rendues par des autorités administratives fédérales ou, plus rarement, par des cours cantonales.
GAFAM: acronyme formé des initiales des multinationales américaines Google, Apple, Facebook, Amazon et Microsoft. Ces dernières sont considérées comme des géants de la technologie numérique, et dominent le marché occidental.
BATX: acronyme inspiré du modèle GAFAM et transposé aux géants chinois de la technologie: Baidu, Alibaba, Tencent et Xiaomi.

Introduction

Le présent mémoire s'intéresse aux problématiques juridiques posées par le cloud computing en matière de protection des données en Suisse.

Au chapitre 1, le concept de cloud computing, ainsi que les notions et terminologies afférentes, sont définis. Une fois les bases techniques introduites, le régime juridique suisse en matière de protection des données ainsi que les enjeux relatifs au cloud computing sont abordés dans les chapitres 2 et 3. Des propositions de mesures juridiques et techniques visant à assurer des services de cloud conformes à la législation y sont alors émises. Finalement, le chapitre 4 constitue un casus permettant la mise en application pratique de la théorie juridique. Il porte sur l'étude de la compatibilité du projet de cloud fédéral *Public Clouds Confederation* avec le droit suisse en matière de protection des données pour les personnes physiques.

1. Définition du cloud computing

L'expression cloud computing peut se traduire en français par "l'informatique en nuage", mais l'usage de l'expression anglaise est courant [1] et est ici employé.

Le cloud computing est la pratique informatique permettant un accès à distance par réseau (Internet ou VPN) à un riche éventail de services informatiques tels que du stockage de données, des serveurs, des outils de calculs ou des logiciels [2, 3].

Il est possible de distinguer trois principaux types de services cloud :

a) l'infrastructure en tant que service (IaaS) : le fournisseur met à disposition, via le cloud, l'infrastructure matérielle (à l'instar de serveurs) sur lequel le client peut héberger ses applications et ses données [4]. *Exemples d'IaaS : Amazon EC2, Google Compute Engin*e.
b) la plateforme en tant que service (PaaS) : le fournisseur rend disponible via le cloud l'infrastructure matérielle ainsi que des applications de base (comme le système d'exploitation ou la base de données). Le client peut ensuite héberger ou développer des applications sur le cloud, ainsi que traiter des données à distance [4, 5, 6]. *Exemples de PaaS : OpenShift, Windows Azure.*
c) le logiciel en tant que service (SaaS) : le prestataire opte pour la mise à disposition d'un logiciel sur le cloud plutôt qu'en local sur des machines. L'utilisateur du logiciel communique avec celui-ci à travers une interface client aisément accessible par un navigateur (Chrome, Safari, Firefox, etc.) ou par une interface logicielle dédiée. L'utilisateur ne peut bénéficier que des fonctionnalités prédéfinies par le prestataire et n'a à priori pas de prétention en termes de configuration du cloud [4, 5]. *Exemples de SaaS : Microsoft 365, Dropbox.*

La répartition de la maîtrise du système informatique entre le prestataire et l'utilisateur dépend donc du type de service cloud (cf. figure n°1). Pour le fournisseur de cloud, la maîtrise est minimale dans le cadre d'un IaaS (première couche de virtualisation du cloud), s'étend dans le cadre d'un PaaS et se révèle maximale pour un SaaS. Les enjeux de sécurité ou de responsabilité entre le prestataire et l'utilisateur varient par conséquent en fonction du type de service cloud offert.

[1] FANTI Sébastien, 2013, p.74.
[2] Périodique CANTON-COMMUNES, 2022.
[3] RUFENER, Adrian, 2013, p.297.
[4] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.
[5] Everwin, 2022.
[6] MELL, Peter et GRANCE, Timothy, NIST, 2011, p.2-3.

D'après le National Institute of Standards and Technology (NIST) [7], il existe en outre quatre modèles de déploiement de ces services cloud :

a) le cloud privé : l'usage du cloud est réservé exclusivement à un utilisateur déterminé. La propriété, la gestion ou l'exploitation du cloud peuvent être exercées par la personne utilisatrice, par un fournisseur tiers ou par une combinaison des deux. Le service cloud est configuré selon les exigences de la personne bénéficiaire et répond au mieux à ses attentes [7, 8].
b) le cloud public : l'utilisateur ne possède pas la jouissance exclusive du cloud qui est accessible en usage ouvert au public. A ce titre, l'utilisateur n'est qu'un client parmi de nombreux autres et ne peut généralement pas personnaliser la configuration du cloud. Il souscrit aux conditions imposées par le fournisseur. Le cloud est entièrement détenu, géré et exploité par le prestataire [7, 8].
c) le cloud communautaire : l'usage du cloud est réservé exclusivement à une communauté de personnes qui partagent les mêmes préoccupations (en termes d'objectifs ou d'exigences de sécurité par exemple). Le cloud est configuré selon les besoins de la communauté. Il est détenu, géré et exploité par un ou plusieurs membres de la communauté, par un fournisseur tiers, ou une combinaison des deux [7].
d) le cloud hybride : plusieurs cloud distincts, qu'ils soient privés, publics ou communautaires, sont reliés entre eux, tout en gardant leurs caractéristiques individuelles. La portabilité des données et des applications est assurée [7].

Finalement, il existe de multiples variantes de clouds. Certaines opèrent à l'aide de datacenters dont la localisation est bien déterminée, d'autres vont jusqu'à séparer logiquement voire physiquement les données de l'utilisateur [9].

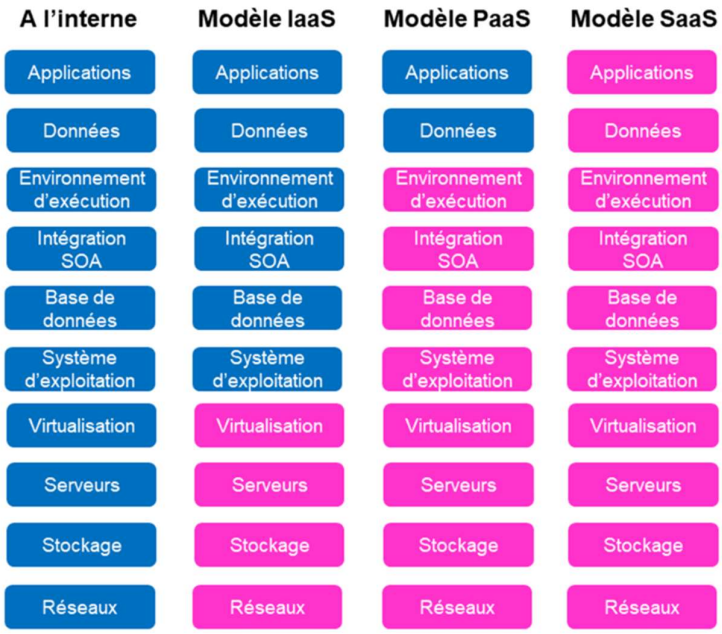

Figure n°1 : répartition de la maîtrise du système informatique entre fournisseur (rose) et utilisateur (bleu), image extraite de la page de l'État de Vaud au sujet du cloud computing [10]

[7] MELL, Peter et GRANCE, Timothy, NIST, 2011, p.3.
[8] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.
[9] METILLE, Sylvain, 2019, p. 610.
[10] Périodique CANTON-COMMUNES, 2022.

Pour conclure, les avantages du cloud computing sont nombreux : accès à distance, mobilité, flexibilité, standardisation de l'environnement informatique, accès à des capacités dynamiques de stockage ou de traitement jusqu'alors inabordables, réduction des coûts d'infrastructure informatique et de logiciels, ou encore mise à jour des applications [11, 12, 13]. Depuis une décennie, d'innombrables personnes physiques, entreprises, autorités et institutions ont ainsi recouru au cloud computing, faisant traiter ou héberger des données et applications, jadis évoluant en interne, sur des serveurs décentralisés.

Bien que les bénéfices apportés par le cloud computing soient indéniables, ils ne doivent pas conduire à éclipser les écueils sécuritaires et juridiques générés par la délocalisation des applications, des données et du traitement de données. Les risques encourus doivent être clairement connus et statués par les différentes parties impliquées. Il s'agit notamment d'éviter le recours à des pratiques jugées contraires à la législation et engageant la responsabilité, ou l'exposition à des menaces trop élevées. L'étude des enjeux juridiques et sécuritaires relatifs au cloud computing fait l'objet de ce mémoire.

2. Régime juridique suisse en matière de protection des données et cloud computing

Le régime juridique suisse en matière de protection des données vise à garantir le droit de la personnalité et les droits fondamentaux des personnes dont les données sont traitées. Il participe ainsi à concrétiser le droit à la protection de la personnalité régi aux articles 28ss du Code civil suisse du 10 décembre 1907 (Code civil, CC ; RS 210), et le droit à la protection de la sphère privée consacré à l'article 13 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Constitution, Cst ; RS 101) [14].

La législation fédérale en matière de protection des données est constituée par :

- la Loi fédérale sur la protection des données du 19 juin 1992 (Loi sur la protection des données, LPD ; RS 235.1),
- l'Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (Ordonnance sur la protection des données, OLPD ; RS 235.11),
- l'Ordonnance sur les certifications en matière de protection des données du 28 septembre 2007 (Ordonnance sur les certifications en matière de protection des données, OCPD ; RS 235.13).

La LPD, l'OLPD et l'OCPD ont fait dernièrement l'objet de révisions complètes qui entreront en vigueur au 1er septembre 2023. C'est à l'aune de la nouvelle Loi fédérale sur la protection des données du 25 septembre 2020 (nouvelle Loi sur la protection des données, nLPD ; RS 235.1) ainsi que de son Ordonnance du 25 septembre 2020 (nouvelle Ordonnance sur la protection des données, nOPDo ; RS 235.11) que la protection des données est par conséquent étudiée dans ce mémoire.

Il est à noter que la protection des personnes morales n'est plus couverte par la nLDP (sous réserve de la période transitoire de 5 ans prévue à l'art. 71, nLPD). Cela s'explique notamment par une volonté d'harmonisation du législateur avec le nouveau Règlement européen sur la protection des données (RGPD) entré en application le 25 mai 2018 dans l'ensemble de l'Union européenne [15, 16].

La personnalité des personnes morales, dont les données sont traitées, reste néanmoins protégée par diverses dispositions légales en vigueur actuellement ou prochainement, comme :

- les articles 28ss, CC, constituant le régime général protégeant la personnalité [17],

[11] FANTI, Sébastien, 2013, p.74-75.
[12] RUFENER, Adrian, 2013, p.298.
[13] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.
[14] METILLE, Sylvain, 2021, p. 5.
[15] HUSSAIN, Zarmine et CHUFFART-FINSTERWALD, Stéphanie, sigma legal SA, 2023.
[16] Confédération suisse, portail PME, *Nouvelle loi sur la protection des données (nLPD)*, 2022.
[17] METILLE, Sylvain, 2021, p. 4.

- les articles 320 et 321 du Code pénal suisse du 21 décembre 1937 (Code pénal, CP ; RS 311.0) en son état du 1er septembre 2023, sanctionnant la violation du secret de fonction et du secret professionnel,
- la Loi fédérale du 9 octobre 1992 sur le droit d'auteur et les droits voisins (Loi sur le droit d'auteur, LDA ; RS 231.1) [18],
- la Loi fédérale du 19 décembre 1986 contre la concurrence déloyale (Loi contre la concurrence déloyale, LCD ; RS 241) [18,]
- les articles 57s et 57t de la Loi fédérale du 21 mars 1997 (en l'état futur du 1er septembre 2023) sur l'organisation du gouvernement et de l'administration (Loi sur l'organisation du gouvernement et de l'administration, LOGA ; RS 172.010) relatifs à la communication des données et aux droits des personnes morales [18].

Bien que l'attirail législatif garantissant la protection des données des personnes morales ait été brièvement abordé ici dans un souci d'information du lecteur, aucune analyse supplémentaire concernant les éléments en lien avec le cloud computing ne sera effectuée par nécessité de simplification. Il est également à noter que le régime juridique en matière de protection des données personnelles traitées par des organes cantonaux ou communaux n'est pas non plus examiné dans le cadre de ce travail, en raison de la trop grande diversité de ses composantes. Par conséquent, le présent mémoire se concentre uniquement sur la protection des personnes physiques dont les données sont traitées dans le cloud par des personnes privées ou des organes fédéraux, visée par la nLPD.

3. Protection des données des personnes physiques (nLPD) et cloud computing

Un protocole, sous forme d'une série de questions à réponse binaire oui/non, est ici proposé pour apprécier la conformité globale d'un service cloud avec les dispositions principales de la nLPD. Sur cette base, un logigramme simplifié est établi à la fin de ce chapitre (cf. figure n°2, en page 20).

3.1. Champ d'application matériel, personnel et territorial de la nLPD (art. 2, 3 et 5, nLPD)

Au sens de l'art. 2, al. 1, nLPD, n'importe quel cloud opérant un traitement de données personnelles, concernant des personnes physiques, sous la responsabilité de personnes privées ou d'organes fédéraux, est soumis à la nLPD. Sont néanmoins réservées les exceptions prévues à l'art. 2, al. 2, 3 et 4, nLPD.

La notion juridique de traitement est large et englobe la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données (art. 5, let. d, nLPD). L'écrasante majorité des opérations effectuées sur le cloud peut donc être assimilée à un traitement au sens juridique. Par données personnelles, le législateur entend toutes les informations concernant une personne physique identifiée ou identifiable (art. 5, let. a, nLPD). Un cloud traitant des données préalablement chiffrées, non identifiables par le prestataire, n'est donc pas soumis à la nLPD. Si un tel chiffrement est envisageable dans le cas d'un simple hébergement de données, il est en revanche irréalisable en cas d'utilisation d'applications sur le cloud nécessitant l'accès aux données claires [19]. Finalement, par responsable du traitement, la loi entend "la personne privée ou l'organe fédéral qui (…) détermine les finalités et les moyens de traitements des données" (art. 5, let. j, nLPD).

En sus de ce champ d'application matériel et personnel, la nLPD possède un large champ territorial. En effet, elle s'applique aux états de fait se produisant aussi bien en Suisse qu'à l'étranger, et susceptibles d'engendrer des effets sensibles en Suisse (art. 3, al. 1, nLPD). Le responsable du traitement ou le prestataire cloud gérant les données de personnes physiques, résidantes en Suisse, sont ainsi assujettis à

[18] HUSSAIN, Zarmine et CHUFFART-FINSTERWALD, Stéphanie, sigma legal SA, 2023.
[19] METILLE, Sylvain, 2019, p. 615.

la nLPD, indépendamment de la localisation de leur domicile ou du for logiciel et infrastructurel du traitement, pourvu que des effets sensibles soient possiblement occasionnés sur le territoire suisse.

ÉTAPE 1 : Le traitement dans le cloud est-il soumis à la nLPD ?

- ⇨ **1.1)** le cloud opère-il un traitement au sens juridique (art. 2, al. 1 et art. 5, let. d, nLPD) ?
- ⇨ **1.2)** le traitement dans le cloud concerne-t-il des données personnelles (identifiées ou identifiables) de personnes physiques (art. 2, al. 1 et art. 5, let. a et b, nLPD) ?
- ⇨ **1.3)** le responsable du traitement est-il une personne privée, établie en Suisse ou à l'étranger, ou un organe fédéral (art. 2, al. 1, nLPD) ?
- ⇨ **1.4)** le traitement dans le cloud s'oppose-t-il aux exceptions prévues au champ d'application de la nLPD (art. 2, al. 2, 3 et 4, nLPD)
- ⇨ **1.5)** le traitement dans le cloud est-il susceptible d'engendrer des effets sensibles sur la personnalité des personnes physiques résidentes en Suisse (art. 3, al.1, nLPD) ?

Si 5x OUI, le traitement dans le cloud est soumis à la nLPD

Si 1x NON, le traitement dans le cloud n'est pas assujetti à la nLPD

3.2. Principes érigés dans la nLPD (art. 6, nLPD), à respecter lors du traitement dans le cloud

a) La licéité

En vertu de l'article 6, al. 1, nLPD, un traitement de données doit être licite. Conformément à la jurisprudence du TAF, la licéité d'un traitement correspond au respect, par ce dernier, de l'ensemble des normes juridiques suisses visant à protéger la personnalité [20].

D'après le préposé fédéral à la protection des données et à la transparence (PFPDT), les entreprises et les autorités, responsables de traitement, qui recourent à des services clouds n'ont toutefois "souvent pas pleinement conscience qu'elles répondent principalement du respect des règles (…), et non le prestataire qui enregistre les données" [21]. Par conséquent, le responsable d'un traitement doit être soucieux d'agir licitement, c'est-à-dire conformément à l'ensemble de ses obligations légales en matière de protection des données lorsqu'il fait usage d'un service cloud.

A titre illustratif, il est possible d'évoquer l'obligation légale relative à la sauvegarde d'un secret de fonction ou d'un secret professionnel imposée au responsable d'un traitement de données (art. 320 et 321, CP et art. 62, nLPD). Cela peut par exemple être le cas pour l'autorité fiscale qui traite les données personnelles des contribuables ou pour l'avocat qui traite celles de ses clients. Comme l'explique Sylvain Métille (2019), rien ne s'oppose à priori à ce que le responsable d'un tel traitement recourt à un prestataire cloud externe pour sous-traiter des données secrètes pour peu qu'il observe certaines précautions. Il doit notamment s'assurer au préalable de la qualité légale d'auxiliaire du prestataire cloud au sens de l'article 320 ou 321, CP. Le prestataire de cloud (l'auxiliaire) devient alors astreint, à son tour, au devoir de sauvegarde du secret. Même si le fournisseur de cloud semble jouir de cette qualité légale d'auxiliaire, il est fortement recommandé pour le responsable du traitement de conclure un contrat pour s'assurer que le prestataire sera effectivement tenu au secret [22]. Néanmoins, dans le cas où le secret est communiqué sur des clouds à l'étranger, le respect du devoir de sauvegarde par le prestataire n'est pas toujours garantissable, puisque ce dernier peut avoir à répondre prioritairement au droit étranger. De manière similaire, un prestataire dont le siège se trouve dans un pays donné, peut-être soumis à des obligations envers les autorités dudit pays, et ce indépendamment de la localisation de ces activités de

[20] ATAF-3548/2018.
[21] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.
[22] METILLE, Sylvain, 2019, p. 613.

traitement (entendre par là de ses datacenters). C'est notamment le cas des États-Unis avec le *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) qui oblige un prestataire cloud y siégeant à transmettre des données personnelles sur requête des autorités [23]. Pour résumer, le responsable d'un traitement, soumis au secret peut sous-traiter ses données secrètes dans le cloud mais il doit s'assurer au préalable, légalement et contractuellement, que les données soient communiquées à des tiers assujettis au devoir de sauvegarde. Le domicile du fournisseur de cloud et le lieu de traitement des données (des datacenters) doivent de plus se situer dans un pays adéquat (cf. p. 15). Dans le cas contraire, les données communiquées à l'étranger ou à des entreprises étrangères devraient être chiffrées, ou bien le consentement de la personne titulaire du secret recueillie. Si l'ensemble de ces conditions ne sont pas satisfaites, la sauvegarde du secret n'est pas garantie, et le recours au service cloud doit être évité, sous peine d'illicéité commise par le responsable du traitement.

b) La proportionnalité et la bonne foi

L'article 6, al. 2, nLPD, consacre le principe de proportionnalité et de bonne foi devant gouverner un traitement de données. Il implique que le traitement effectué par le responsable du traitement soit indispensable au but visé, prompt à produire les résultats escomptés et proportionné au sens étroit, c'est-à-dire raisonnable du point de vue de la personne concernée [24].

En transposant le principe de proportionnalité au cloud computing, cela impliquerait par exemple que le responsable d'un traitement ou le prestataire d'un service cloud, notamment SaaS, se restreigne à collecter, utiliser, enregistrer ou encore archiver dans le cloud uniquement les données nécessaires au traitement convenu (principe de minimisation des données). Les moyens employés pour atteindre le but du traitement devraient aussi être adéquats et minimiser les risques pour la personnalité des personnes physiques concernées. Par exemple, s'il est alternativement possible pour une personne privée ou un organe fédéral d'atteindre les finalités du traitement avec des ressources internes, à moindre coût, et pour un niveau de sécurité supérieur, le recours à un service de cloud externe pour traiter des données ne semble pas légitimé. De même, plus les données sont susceptibles d'engendrer des atteintes à la personnalité, plus les mesures sécuritaires doivent être strictes. Suivant cette logique de proportionnalité, le législateur a ainsi interdit la communication de données sensibles (art. 5, let. c, nLPD et art. 30, al. 2, let. c, nLPD), dans un cloud externe par exemple, en l'absence de motifs justificatifs comme le consentement de la personne concernée (art. 31, al. 1, nLPD et art. 36, al. 2, let. b, nLPD), un intérêt privé ou public prédominant (art. 31, al. 1 et 2, nLPD et art. 36, al. 2, let. a et c, nLPD), ou une base légale (art. 31, al. 1, nLPD et art. 34, al. 1, nLPD). Le principe de proportionnalité s'applique également à d'autres domaines à l'instar de la durée de conservation des données (art. 6, al. 4, nLPD) ou des conditions de recours à un fournisseur externe par des organes fédéraux, telles que listées aux articles 8ss de l'Ordonnance fédérale du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (Ordonnance sur la transformation numérique et l'informatique, OTNI ; RS 172.010.58). Ces deux cas seront évoqués ultérieurement.

c) La reconnaissabilité

L'article 6, al. 3, nLPD, consacre le principe de reconnaissabilité d'un traitement de données (aussi appelé principe de transparence). Ce principe prévoit que la personne dont les données sont traitées soit informée au préalable de la collecte de ses données et de la finalité du traitement, sauf si une loi ou les circonstances autorisent le traitement [25]. D'après David Rosenthal (2020) [24], l'alinéa 3 n'impose pas au responsable de faire connaître les autres paramètres du traitement à la personne concernée. Ainsi, le

[23] METILLE, Sylvain, 2019, p.614.
[24] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.15.
[25] METILLE, Sylvain, 2021, p. 10-11.

principe de reconnaissabilité ne supposerait pas que le recours à un service cloud par une personne privée ou un organe fédéral soit nécessairement notifié à la personne dont les données sont traitées.

Néanmoins, d'autres dispositions prévues par la nLPD imposent au responsable d'un traitement d'informer la personne concernée du recours à une pratique de cloud computing. En particulier, le principe de proportionnalité et de bonne foi évoqué précédemment (art. 6, al. 2, nLPD) implique que la personne concernée soit informée des paramètres importants d'un traitement, à l'instar du recours au cloud, dans la mesure où ladite personne présente un intérêt vraisemblable à l'être [26] (et que l'usage d'un service cloud ne ressorte ni de la loi, ni des circonstances). En vertu du principe de proportionnalité et de bonne foi, il est par exemple possible de déduire qu'un cabinet d'avocats ou de médecins souhaitant héberger dans un cloud public SaaS des données de ses clients ou patients devrait en informer les personnes concernées. En effet, le recours au cloud computing ne semblerait pas correspondre, dans le cas d'espèce, à "la marche normale des affaires". Les personnes concernées auraient alors un intérêt personnel à savoir que des données sensibles, confidentielles ou secrètes puissent être délocalisées sur le cloud. Sur la base de cette information, elles pourraient consentir de manière éclairée au traitement dans le cloud, après avoir apprécié les risques posés à la protection de leurs données. L'article 19, nLPD, discuté plus tard dans ce mémoire, exige également du responsable un devoir d'informer lors de la collecte de données personnelles. Toujours selon David Rosenthal (2020) [26], la disposition de l'article 19, nLPD, est à différencier de l'article 6, nLPD, en ce qu'elle est de nature publique, là où le principe de proportionnalité concrétise la protection de la personnalité régie aux articles 28 CC.

d) La finalité

Le principe de finalité peut être perçu comme un prolongement du principe de proportionnalité dans sa dimension temporelle [25]. Il prescrit au responsable du traitement de détruire ou d'anonymiser les données (les rendre impersonnelles), une fois que celles-ci ne se révèlent plus nécessaires aux finalités primaires ou secondaires du traitement. Afin d'assurer la mise en application du principe de finalité, le Conseil fédéral a ordonné au responsable d'un traitement de fixer des délais de conservation des données [27].

Or, recourir au cloud peut se révéler être un obstacle au respect de cette obligation. En effet, le PFPDT a identifié la perte de contrôle du responsable du traitement sur les données comme l'un des risques du cloud computing. Il énonce que "l'interconnexion mondiale et l'utilisation de la mémoire virtuelle font qu'il est souvent impossible de localiser les données, notamment lorsqu'on a recours à des nuages publics. Le maître des données ne sait donc pas où les données qu'il a déposées dans le nuage sont enregistrées et traitées alors qu'il répond de leur utilisation. (…). L'utilisateur d'un nuage ne peut donc pas assumer ses obligations en matière de protection des données (garantir la sécurité des données, accorder un droit d'accès, corriger ou effacer des données) ou uniquement en partie" [28]. Par conséquent le responsable du traitement doit s'assurer qu'il sera effectivement en mesure d'effacer ou anonymiser les données évoluant dans le cloud au terme du délai de conservation. Dans la pratique, une telle vérification peut s'avérer complexe. Il semble donc judicieux que le prestataire cloud garantisse contractuellement au responsable du traitement la maîtrise sur les données en tout temps. Si tel n'est pas le cas, le recours au cloud ne semble pas indiqué pour le responsable du traitement.

e) L'exactitude

Le principe d'exactitude des données édicté à l'art. 6, al. 5, nLPD, stipule que le responsable du traitement doit s'enquérir de l'exactitude des données traitées, mais uniquement au regard de la finalité

[26] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.15-16.
[27] FF 2017 6565.
[28] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.

de traitement. Le cas échéant, le responsable doit prendre les mesures qui s'imposent (effacement, destruction ou rectification de données). Ces mesures doivent cependant être de nature appropriée et répondre au principe de proportionnalité [29].

Comme pour le principe de finalité, la problématique du risque de perte de contrôle du responsable du traitement sur les données situées dans le cloud intervient si ce dernier devait effacer, détruire ou rectifier des données. Là encore, il est primordial qu'une clause contractuelle garantisse au responsable la maîtrise sur les données en tout temps. Si tel n'est pas le cas, le recours au cloud est déconseillé car la responsabilité juridique du responsable du traitement pourrait être engagée (art. 32, nLPD).

f) Le consentement

Le dernier principe que la nLPD consacre à l'article 6, alinéas 6 et 7, est celui de la validité du consentement dans le cadre d'un traitement de données. Il est important de noter que les alinéas 6 et 7 ne précisent pas si le consentement est en général requis lors d'un traitement de données, et encore moins les cas pour lesquels il serait nécessaire. Les alinéas 6 et 7 se limitent strictement à énoncer les conditions pour lesquelles le consentement doit être considéré comme valide [30].

La première condition de validité du consentement de la personne concernée quant au traitement de ses données consiste, au sens de l'art. 6, al. 6, nLPD, en une expression libre et dûment informée du consentement. D'après Philippe Meier (2011) [31], la terminologie de consentement libre et éclairé, employée ici, est issue de la jurisprudence applicable en droit médical. Le consentement peut être considéré éclairé lorsque la personne concernée l'exprime sur la base d'une information objective, complète et compréhensible [32]. Cela suppose que le type de données traitées (sensibles ou classiques) ainsi que les méthodes de traitements envisagées (cloud externe ou ressource interne) soient connus de la personne concernée au moment de son approbation. Le consentement peut être considéré libre lorsqu'il intervient en l'absence de menace ou d'une pression déraisonnable. Dans le cadre du recours à un service cloud, il est possible d'imaginer deux situations susceptibles de conduire à un état de fait assimilable à une pression déraisonnable pour la personne concernée, prétéritant son droit à un consentement absolument libre. La première situation serait la captivité que subissent certains utilisateurs de services cloud. Ce risque de captivité a par ailleurs été clairement identifié par le PFPFT qui affirme : "les utilisateurs peuvent devenir dépendants du prestataire en raison de la faible portabilité et de la faible interopérabilité des services en nuage. En effet, si le prestataire n'a pas recours à une technologie et à une interface standardisée, le rapatriement des données dans le système informatique de l'utilisateur ou leur migration dans le nuage d'un autre prestataire peut être impossible ou extrêmement coûteux" [33]. Il est possible de supposer qu'il est du devoir du prestataire d'offrir une interopérabilité et une portabilité raisonnables des applications et des données évoluant dans le cloud. Dans le cas où le prestataire maintient à dessein ses clients captifs, se constituant ainsi en partie dominante, le consentement de la personne concernée pourrait être jugée invalide à terme. Le prestataire cloud qui traiterait les données des personnes concernées engagerait alors sa responsabilité. Plus largement, de telles pratiques (rendre les utilisateurs captifs) poserait également question d'un point de vue de la concurrence qui doit être loyale et non-faussée entre les différents prestataires de cloud (art. 1, 2, 3, al. 1, let. h, LCD). La deuxième situation hypothétique serait celle du recours injustifié par des personnes privées ou l'administration à des services cloud pour le traitement de données, sans possibilités d'alternatives crédibles. Si le fait de ne pas consentir au recours de ces services cloud présente des

[29] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.17.
[30] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.13-14.
[31] MEIER, Philippe, 2011, N. 831.
[32] METILLE, Sylvain, 2021, p. 36-37.
[33] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.

désagréments considérables et supérieurs au fait de les utiliser pour les personnes concernées ou les administrés, la liberté du consentement est questionnable. Philippe Meier (2011) précise à ce sujet qu'il n'est pas obligatoire de fournir une alternative pour que le consentement soit considéré libre, mais que si une alternative existe, c'est une forte indication de la liberté de consentir [34]. Ajoutons que celui qui consentira au recours à un service cloud public, n'aura souvent pas d'autre choix que d'accepter sans réserve des clauses contractuelles désavantageuses [35].

Finalement, l'art. 6, al. 7, nLPD prescrit la forme expresse pour le consentement lorsqu'il est requis dans le cadre d'un traitement de données sensibles (art. 6, al. 7, let. a et art. 2, let. c, nLPD), d'un profilage à risque élevé effectué par une personne privée (art. 6, al. 7, let. b et art. 2, let. f, nLPD) ou d'un profilage effectué par un organe fédéral (art. 6, al. 7, let. c et art. 2, let. g, nLPD).

ÉTAPE 2 : Le traitement dans le cloud respecte-t-il les principes de la nLPD ?

- ⇨ **2.1)** le traitement est-il licite (art. 6, al. 1, nLPD) ? En particulier, le responsable du traitement observe-t-il toutes ses obligations légales en recourant à un service cloud (exemple du devoir de sauvegarde (art. 320 et 321, CP), du droit de sous-traitance pour l'administration (art., 8ss, OTNI), etc.) ?
- ⇨ **2.2)** le traitement via le cloud respecte-il le principe de proportionnalité au regard du types de données traitées (anodines vs sensibles, etc.) et des moyens de traitement (en local vs cloud externe, etc.) (art. 6, al. 2, nLPD) ? Par ailleurs, la personne concernée est-elle informée du recours au cloud pour traiter ses données, pour autant qu'elle ait un intérêt personnel à l'être ?
- ⇨ **2.3)** le traitement dans le cloud respecte-il le principe de proportionnalité au regard de la durée de conservation des données (art. 6, al. 4, nLPD) ? En particulier, le responsable du traitement est-il effectivement en mesure d'effacer ou d'anonymiser les données dans le cloud le moment venu ?
- ⇨ **2.4)** le traitement dans le cloud permet-il le respect du principe d'exactitude des données (art. 6, al. 5, nLPD) ? En particulier, le responsable du traitement est-il effectivement en mesure de rectifier, effacer ou détruire les données situées dans le cloud si les circonstances l'y poussent ?
- ⇨ **2.5)** si requis, le consentement de la personne concernée au traitement de ses données dans le cloud est-il valide ? En particulier, le consentement est-il libre et éclairé (art. 6, al. 6, nLPD), ainsi qu'expressément prononcé dans le cas d'un traitement de données sensibles, d'un profilage à risque élevé par une personne privée ou d'un profilage par un organe fédéral (art. 6, al. 7, nLPD) ?

Si 5x OUI, le cloud respecte les principes de la nLPD

Si 1x NON, le traitement dans le cloud viole un des principes de la nLPD :

Le responsable du traitement dans le cloud est une personne privée, ou un agit comme tel (art. 40, nLPD) :

- ➢ il y a alors atteinte présumée à la personnalité de la personne concernée (art. 30, al. 2, let. a, nLPD).
- ➢ l'atteinte est réputée illicite si elle n'est pas justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant, ou par la loi (art. 31, al. 1, nLPD).
- ➢ si l'atteinte est illicite, la personne concernée peut alors intenter une action en prévention, en cessation, en constatation ou en rectification. Elle peut en outre demander la publication de la mesure d'action (art. 32, nLPD et art. 28ss, CC).
- ➢ une action en responsabilité civile du responsable du traitement est réservée en cas d'atteinte illicite ayant fautivement causé un dommage à la personne concernée (art. 41, CO).

Le responsable du traitement dans le cloud est un organe fédéral, et agit comme une personne publique :

- ➢ si le traitement dans le cloud est illicite, notamment en raison de l'absence de bases légales suffisantes ou de motifs justificatifs (art. 34 et 36, nLPD), quiconque ayant un intérêt digne de protection peut exiger une action en prévention, en cessation, en constatation ou en rectification de l'atteinte liée au traitement. Il peut en outre demander la publication de la mesure corrective (art. 41, nLPD).

[34] MEIER, Philippe, 2011, N. 859.
[35] FANTI, Sébastien, 2013, p.76.

3.3. Mesures organisationnelles et techniques à observer par le responsable du traitement de données et le prestataire cloud (art. 7 et 8, nLPD, et art. 3, nOPDo)

L'article 7, alinéa 1, nLPD, exige du responsable d'un traitement qu'il mette en œuvre toutes les mesures organisationnelles et techniques permettant le respect des prescriptions en matière de protection des données, en particulier les principes de l'article 6, nLPD, mentionnés précédemment. Ces mesures doivent être implémentées en amont du traitement, dès la phase de conception. C'est l'approche dite du "Privacy by Design". D'après David Rosenthal (2020), ce principe du "Privacy by Design" impose au responsable d'un futur traitement de prospecter l'ensemble des paramètres essentiels au traitement en question [36]. Dans le cas d'un recours au cloud computing, il s'agit notamment d'examiner les différents aspects du service cloud susceptibles d'interférer avec la personnalité des personnes concernées et la sécurité de leurs données. Une fois cette première étape analytique effectuée, le responsable du traitement doit déterminer avec quels moyens il souhaite agir afin de garantir que ses obligations, en matière de protection des données, soient effectivement respectées lors du traitement dans le cloud. Toujours selon David Rosenthal (2020), les moyens à disposition du responsable sont multiples et incluent : "les déclarations de protection des données, les directives internes, la mise en place de possibilités d'opposition, des offres self-service pour l'exercice des droits des personnes concernées, l'utilisation du chiffrement, les processus internes visant à limiter les finalités d'utilisation, la conception des applications de manière à éviter la collecte de données personnelles, l'automatisation de l'effacement des données, les mesures visant à interdire la réidentification, les règles de responsabilité, la documentation des processus, l'évaluation des taux d'erreur à des fins d'assurance qualité, les mesures visant à empêcher les copies de données non synchronisées, et les règles sur la durée de conservation des données" [36]. Les mesures mises en œuvre par le responsable du traitement doivent de plus être conformes à l'état de la technique, appropriées au regard du type de traitement et de son étendue, ainsi que proportionnées au risque encouru pour la personnalité et les droits fondamentaux des personnes concernées (art. 7, al. 2, nLPD). Finalement, l'article 7, alinéa 3, nLPD, ordonne au responsable du traitement de proposer un préréglage axé sur le niveau le plus étroit de protection des données dans le cas où plusieurs options de traitement seraient offertes à l'utilisateur, et que ce dernier ne prête pas son concours à un paramétrage plus étendu. Il s'agit de l'approche du "Privacy by Default" [36]. Par exemple, dans le cas où le responsable d'un traitement recourt à un service cloud et laisse à la personne concernée la possibilité de choisir la localisation des datacenters traitant ses données (en Suisse ou aux États-Unis) ainsi que la variante de cloud déployée (avec ou sans séparation logique des données), le traitement doit être configuré sur l'option la plus respectueuse de la personnalité (dans le cas d'espèce l'option des clouds en Suisse dotés d'une séparation logique des données). Une violation de l'article 7 par le responsable du traitement peut constituer un manquement légal à son devoir de diligence, et donc entraîner sa responsabilité causale au sens de l'article 41, alinéa 1 de la Loi fédérale complétant le Code civil suisse du 30 mars 1911 (Code des obligations, CO ; RS 220).

En complément à l'article 7, nLPD, l'article 8, alinéa 1, exige du responsable du traitement ainsi que du prestataire de service cloud externe, qui est un sous-traitant au sens de l'art. 9, nLPD (cf. p.13) la mise en œuvre de mesures techniques et organisationnelles propres à assurer la sécurité adéquate des données à l'égard des risques encourus. Les mesures prises doivent également être conformes à l'état de la technique. L'article 8 se distingue de l'article 7, nLPD, en ce qu'il s'applique aussi au prestataire cloud, et qu'il vise uniquement la protection des données personnelles d'un point de vue de leur sécurité. D'après l'art. 3, OPDo, la sécurité des données se décline en trois composantes : la confidentialité (accès aux données limité à des personnes définies), l'intégrité (protection des données contre les manipulations

[36] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.22-25.

préjudiciables) et la disponibilité (données disponibles sous une forme voulue) [37, 38]. Lors du recours au cloud computing, la sécurité des données peut être menacée par différents risques, comme les pertes de données, l'usage abusif des données, les pannes de système, les pannes de réseau, la non-disponibilité des ressources et des services, la perte de contrôle ou le manque de séparation et d'isolation des données dans les serveurs [39]. Le responsable du traitement doit donc mettre en œuvre des mesures techniques et organisationnelles proportionnées au niveau et à la nature de ces risques sécuritaires, de manière à limiter raisonnablement la probabilité d'une violation de la sécurité des données (art. 8, al. 2, nLPD). La notion de proportionnalité de la mesure implique par exemple que plus les données présentent un caractère sensible, secret ou confidentiel, moins un déport sur le cloud devrait être privilégié, et plus les mesures de sécurité et de contrôle devraient être strictes [39]. D'après David Rosenthal (2020), les mesures traditionnelles permettant de gérer les risques sécuritaires incluent notamment les restrictions d'accès, les filtres, la pseudonymisation, le chiffrement, l'enregistrement, les sauvegardes, les techniques d'élimination sécurisée, la surveillance, les systèmes d'alarme, les règlements et directives, la formation, la sélection de sous-traitants, les contrats régissant le traitement ou la confidentialité des données, la documentation, les contrôles, les tests d'intrusion et les règles de responsabilité [37]. Il est possible d'ajouter à cette liste d'autres mesures davantage spécifiques au cloud computing, comme le choix d'une architecture cloud favorisant la sécurité (séparation logique et physique des données), le recours à un cloud privé encourageant la négociation de clauses contractuelles à l'avantage de l'utilisateur, le traitement de données dans des clouds situés dans des pays adéquats, la sélection de prestataires dont le siège se situent dans des pays adéquats, ou encore la préférence d'un traitement en local pour les données sensibles, confidentielles ou secrètes. Peu importe les mesures qu'il entreprend, le responsable du traitement a le devoir d'observer les exigences minimales en matière de sécurité promulguées par le Conseil fédéral (art. 8, al. 3, nLPD).

ÉTAPE 3 : Le responsable du traitement et le prestataire cloud observent-ils les mesures techniques et organisationnelles permettant la protection et la sécurité des données traitées dans le cloud ?

- ⇨ **3.1)** le responsable du traitement a-t-il appliqué l'ensemble des mesures techniques et organisationnelles propres à assurer la protection des données traitées dans le cloud, dès la conception et par défaut, conformément à l'état de la technique (art. 7, nLPD) ?
- ⇨ **3.2)** le responsable du traitement et le prestataire cloud ont-t-il appliqué l'ensemble des mesures techniques et organisationnelles propres à assurer la sécurité des données traitées dans le cloud, conformément à l'état de la technique (art. 8, nLPD) ?

Si 2x OUI, la protection et la sécurité des données est garantie au sens de la nLPD

Si 1x NON, la protection et la sécurité des données n'est pas garantie au sens de la nLPD

Le responsable du traitement ou le prestaire cloud agit comme une personne privée :

- ➢ il y a alors atteinte présumée à la personnalité de la personne concernée (art. 30, al. 2, let. a, nLPD). La même réflexion logique qu'à l'étape 2 s'ensuit.
- ➢ les personnes privées, responsables du traitement dans le cloud, qui, par dol, ne respectent pas les exigences sécuritaires minimales édictées à l'art. 8, al. 3, nLPD, s'exposent, sur plainte, à une amende de 250'000 francs (conformément à l'art. 61, let. c, nLPD).
- ➢ une action en responsabilité civile du responsable du traitement est réservée en cas d'atteinte illicite ayant fautivement causé un dommage à la personne concernée (art. 41, CO).

Le responsable du traitement est un organe fédéral, agissant comme une personne publique :

- ➢ si le traitement dans le cloud est illicite, notamment en raison de l'absence de bases légales suffisantes ou de motifs justificatifs (art. 34 et 36, nLPD), quiconque ayant un intérêt digne de protection peut exiger une action en prévention, en cessation, en constatation ou en rectification de l'atteinte liée au traitement. Il peut en outre demander la publication de la mesure corrective (art. 41, nLPD).

[37] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.22-25.
[38] METILLE, Sylvain, 2019, p. 610-611.
[39] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.

3.4. Conditions à la sous-traitance du traitement de données dans le cloud (art. 9, nLPD)

Le cas de l'externalisation, par le responsable du traitement (personne privée ou organe fédéral), des fonctions informatiques à un prestataire cloud, constitue un acte de sous-traitance au sens de l'art. 9, nLPD. Cette sous-traitance est en principe autorisée par la nLPD et ne requiert pas le consentement de la personne concernée. Néanmoins, et comme évoqué précédemment (cf. p. 7-9), cette externalisation doit être proportionnée, faute de quoi la personne concernée devrait être dûment informée et son consentement recueilli [40].

Pour être licite, la sous-traitance dans le cloud doit cependant satisfaire à certaines conditions élémentaires listées à l'article 9, nLPD.

L'article 9, alinéa 1, nLPD, autorise ainsi le responsable du traitement à déléguer le traitement des données à un prestataire externe à condition que la loi ou qu'un contrat le prévoie. Par ailleurs, le prestaire cloud (le sous-traitant) est uniquement habilité à réaliser des traitements que le responsable lui-même serait en droit d'effectuer (art. 9, al. 1, let. a, nLPD). De plus, le responsable du traitement doit s'assurer qu'aucune obligation légale ou contractuelle à la sauvegarde d'un secret ne s'oppose à la sous-traitance dans le cloud (art. 9, al. 1, let. b, nLPD), comme mentionné antérieurement (cf. p. 6 et 7).

Additionnellement, l'article 9, alinéa 2, nLPD, exige du responsable du traitement qu'il s'assure *in concreto* de la capacité effective du sous-traitant (le prestataire cloud) à garantir la sécurité des données. Dans les faits, une telle vérification peut s'avérer difficile pour le responsable du traitement, en raison notamment de la délocalisation des données, de la mondialisation et de la virtualisation du réseau, de la dématérialisation de l'architecture informatique, ou encore de l'opacité régnant chez certains prestataires externes. Ce processus de vérification est cependant primordial puisque c'est le responsable du traitement qui répond prioritairement de toute violation de la sécurité des données à l'égard des personnes concernées (tout en disposant d'actions récursoires envers le prestataire). Le responsable du traitement doit donc sélectionner scrupuleusement le prestataire de cloud en effectuant une analyse des risques organisationnels, juridiques et techniques. Idéalement, il devrait également pouvoir négocier des clauses contractuelles personnalisées, propres à garantir la sécurité des données dans le cloud externe, être en mesure de donner des instructions au prestataire ainsi que procéder à des contrôles *in-situ* ponctuels [41, 42]. En cas de sous-traitance dans des services clouds publics, le responsable du traitement bénéficie toutefois rarement d'une possibilité de négociation contractuelle, d'un droit de contrôle ou d'un droit d'instruction. En effet, le responsable du traitement, n'étant qu'un client parmi de multiples autres, est fréquemment obligé d'accepter des clauses désavantageuses [43]. Individuellement, la marge de négociation n'existe donc pas. De plus, un prestataire cloud n'autorise généralement pas le responsable du traitement à effectuer ses propres contrôles. Dans le meilleur des cas, le prestataire préférera souvent mandater des sociétés d'audits indépendants, délivrant des certificats, servant de gage de qualité de protection des données (voir art. 13, nLPD). Quant au droit d'instruction, il se limite généralement aux instructions convenues contractuellement ou livrées par le responsable du traitement lors de la configuration du cloud [44]. S'il en résulte que le responsable du traitement n'est pas en mesure de s'assurer de la capacité du sous-traitant à garantir la sécurité des données, il devrait renoncer au cloud externe. S'il persiste tout de même à sous-traiter le traitement des données et applications, il violerait

[40] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.25.
[41] METILLE, Sylvain, 2019, p. 610-611.
[42] PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.
[43] FANTI, Sébastien, 2013, p.76.
[44] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.26.

délibérément l'obligation découlant de l'art. 9, al. 2, nLPD, et engagerait sa responsabilité pénale. Il s'exposerait alors à une amende de 250'000 francs conformément à l'art. 61, let. b, nLPD.

Finalement, l'article 9, alinéa 3, nLPD, proscrit au sous-traitant de sous-traiter à son tour sauf en présence de l'autorisation du responsable du traitement. La forme de cette autorisation est définie contractuellement entre le prestataire cloud et le responsable du traitement. Elle peut être individuelle (tiers nommément connu) ou plus fréquemment générale, avec réserve d'objection. Si l'autorisation est générale, le prestataire cloud est obligé de communiquer au responsable les informations importantes concernant le sous-traitant ultérieur potentiel (identité, pays, etc.). Sur la base de ces informations, le responsable du traitement peut s'opposer au transfert dans un délai de 7 jours à 6 mois [45]. En ce qui concerne l'administration fédérale, les conditions au recours d'un service cloud externe sont légèrement plus strictes que celles imposées aux personnes privées. En effet, les organes fédéraux doivent supplémentairement respecter les dispositions de l'OTNI, notamment l'article 8 prescrivant aux départements et à la Chancellerie fédérale de décider sur la base d'analyse de marché, et en tenant compte des principes d'adéquation, d'interopérabilité, de rentabilité et de sécurité et des exigences en matière de sécurité des données si les prestations informatiques doivent être acquises auprès d'un fournisseur externe. L'article 8, OTNI, en comparaison à l'article 6, al. 2, nLPD, peut être compris comme une concrétisation poussée du principe de proportionnalité. Une autre différence entre l'administration et les personnes privées vient de l'article 11, al. 1, let. b, OTNI, qui prescrit la forme écrite pour la conclusion du contrat de sous-traitance.

ÉTAPE 4 : l'externalisation du traitement de données dans le cloud est-il conforme à la nLPD ?

- ⇨ **4.1)** une loi ou un contrat autorise-t-il la sous-traitance du traitement dans le cloud ? Le traitement effectué par le sous-traitant correspond-il à celui que le responsable du traitement serait en droit de réaliser ? Une obligation légale ou contractuelle à la sauvegarde d'un secret s'oppose-t-elle à l'externalisation du traitement sur le cloud (art. 9, al. 1, nLPD) ?
- ⇨ **4.2)** dans le cas où l'externalisation du traitement dans le cloud n'est pas proportionnée, la personne concernée a-t-elle été informée du recours à un service cloud (art. 6, al. 1, 2, nLPD) ? A-t-elle consenti librement et de manière éclairée au traitement de ses données dans le cloud (art. 6, al. 1, 2, 6, 7, nLPD) ?
- ⇨ **4.3)** de plus, le responsable du traitement s'est-il assuré *in concreto* que le prestataire de cloud externe observe effectivement les mesures sécuritaires prescrites à l'article 8, nLPD (art. 9, al. 2, nLPD) ?
- ⇨ **4.4)** en cas de sous-traitance ultérieure dans le cloud, le responsable du traitement a-t-il donné son autorisation (art. 9, al. 3, nLPD) ?
- ⇨ **4.5)** en cas d'une externalisation du traitement de données dans un cloud par un organe fédéral, la sous-traitance est-elle approuvée en analysant les performances du cloud externe en termes économiques et d'adéquation, d'interopérabilité, de rentabilité et de sécurité et d'exigences en matière de sécurité des données par rapport à d'autres alternatives (art. 6, al. 1, nLPD et art. 8, OTNI) ? De plus, le contrat de sous-traitance a-t-il été conclu en la forme écrite (art. 6, al. 1, nLPD et art. 11, OTNI) ?

Si 5x OUI, la sous-traitance du traitement dans le cloud est licite au sens de la nLPD

Si 1x NON, la sous-traitance du traitement dans le cloud n'est pas conforme à la nLPD

Le responsable du traitement ou le prestaire cloud agit comme une personne privée :

- ➢ les personnes privées, responsables du traitement, qui, par dol, recourent à un prestataire cloud externe sans respecter les conditions de l'art. 9, al. 1 et 2, ou en violation d'un devoir de sauvegarde, s'exposent, sur plainte, à une amende de 250'000 francs (conformément à l'art. 61, let. b, et à l'art. 62, nLPD).
- ➢ une action en responsabilité civile du responsable du traitement est réservée en cas d'atteinte illicite ayant fautivement causé un dommage à la personne concernée (art. 41, CO).

Le responsable du traitement est un organe fédéral, agissant comme une personne publique :

- ➢ si le traitement dans le cloud est illicite (viole notamment les art. 8 et 11, OTNI, sur la sous-traitance), quiconque ayant un intérêt digne de protection peut engager une action au sens de l'article 41, nLPD.

[45] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.27.

3.5. Conditions à satisfaire lors de la communication transfrontalière de données vers le cloud (art. 16ss, nLPD)

Les données ou applications destinées à être traitées dans le cloud doivent très fréquemment être communiquées sur des datacenters situés à l'étranger. Cela s'explique par l'interconnexion des serveurs et la mondialisation du réseau propres au fonctionnement de très nombreux services clouds.

L'article 16, alinéa 1, nLPD, autorise en principe la communication de données personnelles vers des clouds situés dans des États disposant d'une législation assurant un niveau de protection des données jugé adéquat (c'est-à-dire similaire à celui offert par la nLPD en Suisse).

Le caractère adéquat de protection des données, conférée par la législation d'un État étranger, est déterminé par le Conseil fédéral, ou bien garanti par un organisme international (art. 16, al. 1, nLPD). Les appréciations du Conseil fédéral sont inscrites sur une liste du PFPDT, accessible à tous. Le responsable d'un traitement souhaitant communiquer ses données sur un cloud à l'étranger peut donc s'y fier. Néanmoins, il reste responsable de la communication des données et doit quand même s'assurer que le traitement projeté ne s'oppose pas, pour diverses raisons, à la communication vers le pays de destination souhaité. Le responsable du traitement doit aussi vérifier périodiquement le statut d'adéquation de l'État récepteur figurant dans la liste du PFPDT [46].

En l'absence d'une protection adéquate d'un État ou d'indices selon lesquels aucun transfert de données conforme à la protection des données n'y est possible, la communication vers l'État en question reste toujours faisable, moyennant des garanties de protection suffisantes. Ces garanties consistent notamment en des solutions contractuelles ou des règles d'entreprises.

En présence d'une relation externe avec un prestataire cloud à l'étranger, des clauses contractuelles types, appelées *Standard Contract Clauses* (SCC), peuvent par exemple être souscrites entre le responsable du traitement et le prestataire cloud (conformément à l'art. 16, al. 2, let. d, nLPD) [46]. Elles doivent ainsi permettre d'atteindre un niveau de protection des données suffisants dans le cloud. A ce sujet, le PFPDT a reconnu, le 27 août 2021, les clauses contractuelles types pour le transfert de données personnelles vers des pays tiers au sens du règlement (UE) 2016/679 du Parlement européen, à condition qu'elles soient, si nécessaire, adaptées pour être conformes au droit suisse [47].

En présence d'une relation interne à un groupe de sociétés implanté sur le territoire de plusieurs États et échangeant des données (dans un cloud communautaire par exemple), des règles de protection de données internes, appelées *Binding Corporate Rules* (BCR), peuvent également être employées (conformément à l'art. 16, al. 2, let. e, nLPD) [46]. Ces dernières doivent être préalablement approuvées par le PFPDT ou par une autorité chargée de la protection des données relevant d'un État qui assure un niveau de protection adéquat. Dans la pratique, les BCR sont rarement utilisés car ils ne présentent souvent pas d'avantages substantiels par rapport à l'usage de clauses types [48].

D'autres alternatives de garanties aux SCC et BCR existent. Il est par exemple possible pour un exportateur de données d'établir un contrat individuel avec son prestataire de cloud externe (conformément à l'art. 16, al. 2, let. b, nLPD), visant à garantir une protection des données dans le cloud. Le contrat individuel doit être communiqué au préalable au PFPDT, à des fins d'examens et de commentaires [46]. Par analogie, un organe fédéral souhaitant traiter ses données sur un cloud externe à

[46] PFPDT, *Guide pour l'examen de la licéité de la communication transfrontière de données*, 2021, p.3-4.
[47] PFPDT, *Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données requis, en application de clauses contractuelles types et de contrats types reconnus*, 2021, p.3.
[48] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.31-32.

l'étranger peut élaborer des garanties spécifiques, puis les transmettre au PFPDT pour examen et commentaires (art. 16, al. 2, let. c, nLPD). Finalement, le Conseil fédéral se réserve, à l'article 16, al. 3, nLPD, le droit de prévoir d'autres types de garanties. Il peut s'agir de restrictions techniques ou de systèmes d'autocertification, à l'instar de l'ancien *Privacy Shield* [49]. Ce dernier encadrait le transfert de données vers les États-Unis, dont le niveau d'adéquation était jugé adéquat sous cette condition par le Conseil fédéral. Le *Privacy Shield* a été révoqué par le PFPDT le 8 septembre 2020, suivant de peu l'invalidation rendue le 16 juillet 2020 par la Cour de justice de l'Union européenne (CJUE) dans l'affaire C-311/18, dite Schrems II [50]. Les Etats-Unis sont depuis considérés par le PFPDT comme un pays doté d'un niveau insuffisant de protection des données.

Néanmoins, l'ensemble de ces mesures de garanties (contrats types, contrats individuels, règlements, etc.) ne permet pas toujours d'assurer la protection des données communiquées vers un État tiers. En effet, certains États sont dotés de législations permettant à leurs autorités d'accéder aux données situées dans des datacenters s'y trouvant. Il va sans dire que les arrangements contractuels entre l'exportateur de données et le prestataire cloud de l'État tiers ont force nulle pour les autorités en question. Dans ce cas, le cryptage des données, préalable à la communication vers le cloud, peut être une solution apte à garantir la protection ou la sécurité des données. Finalement, la relocalisation du cloud (c'est-à-dire celle des datacenters de traitement et des voies de communication) dans des pays adéquats peut être l'option à privilégier par les personnes privées ou les organes fédéraux, si la communication des données dans les États envisagés ne permet pas la protection et la sécurité des données personnelles [50].

Il est à noter qu'une série de dérogations aux dispositions normant la communication des données personnelles à l'étranger sont énoncées à l'art. 17, nLPD. Ainsi, des données personnelles peuvent être communiquées vers un cloud situé dans des Etats avec un niveau de protection insuffisant si le consentement exprès de la personne concernée a été auparavant recueilli (art. 17, al. 1, let. a, nLPD).

ÉTAPE 5 : la communication transfrontalière des données dans le cloud respecte-elle la nLPD ?

⇨ **5.1)** Les États, dans lesquels les datacenters du cloud opèrent, offrent-ils un niveau adéquat de protection des données pour le traitement en question (au sens de l'art. 16, al. 1, nLPD) ? Si tel n'est pas le cas, les mesures propres à garantir un niveau de protection approprié (clauses contractuelles, règlements internes, chiffrement, etc.) ont-elles été prises par l'exportateur de données (art. 16, al. 2, nLPD) ?

⇨ **5.2)** En cas de communication transfrontalière des données vers des datacenters situés dans des Etats dépourvus de législations adéquates en matière de protection des données, et sans autres mesures de garanties de protection, le cas se rapporte-il à celui d'une dérogation prévue à l'article 17, nLPD (comme le consentement exprès de la personne concernée) ?

Si 2x OUI, la communication transfrontalière des données vers le cloud est conforme à la nLPD

Si 1x NON, la communication transfrontalière des données dans le cloud viole la nLPD

Le responsable du traitement agit comme une personne privée :

- les personnes privées, responsables du traitement, qui, par dol, communiquent des données personnelles à l'étranger en violation de l'art. 16, al. 1 et 2, et sans que les conditions de l'art. 17 soient remplies, s'exposent, sur plainte, à une amende de 250'000 francs (conformément à l'art. 61, let. a, nLPD).
- une action en responsabilité civile du responsable du traitement est réservée en cas d'atteinte illicite ayant fautivement causé un dommage à la personne concernée (art. 41, CO).

Le responsable du traitement est un organe fédéral, agissant comme une personne publique :

- si le traitement dans le cloud est illicite (viole notamment l'art. 16, sans motifs justificatifs), quiconque ayant un intérêt digne de protection peut engager une action au sens de l'article 41, nLPD.

[49] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p.31-32.
[50] PFPDT, *Prise de position sur la transmission de données personnelles vers les États-Unis et d'autres États n'offrant pas un niveau adéquat de protection des données au sens de l'art. 6, al.1 LPD*, 2020, p.4-6.

3.6. Devoir du responsable du traitement d'informer la personne dont les données sont traitées dans le cloud (art. 19ss, nLPD)

En vertu de l'article 19, alinéa 2, lettre c, le responsable d'un traitement est tenu de communiquer à la personne concernée les catégories de destinataires auxquelles ses données personnelles sont transmises. Cela comprend donc les prestataires de clouds externes, qui peuvent être regroupés au sein d'une catégorie "sous-traitants". Les prestataires de services clouds peuvent aussi être désignés et communiqués nommément à la personne concernée, mais le responsable du traitement n'y est pas obligé.

Dans le cas où une communication sur des clouds situés à l'étranger est prévue, les pays de destination et leur niveau d'adéquation en matière de protection des données doivent aussi être portés à la connaissance de la personne concernée (cf. p. 15-16). Selon David Rosenthal (2020), des indications telles que "tous les pays du monde", "dans le monde entier", "en Europe" ou "tous les pays dans lesquels nous sommes représentés" sont acceptés [51]. Dans le cas de figure où les données sont transférées vers un Etat présentant un niveau de protection des données inadéquat, l'article 19, al. 4, nLPD, exige du responsable du traitement qu'il indique également quelles garanties sont prévues ou alors quelles exceptions de l'art. 17 nLPD s'appliquent.

De manière plus générale, le responsable d'un traitement doit communiquer l'ensemble des éléments nécessaires à ce que la personne concernée fasse valoir ses droits au sens de la nLPD, et que la transparence du traitement dans le cloud soit garantie (art. 19, al. 2, nLPD). Selon les circonstances, il peut ainsi être nécessaire de communiquer des informations supplémentaires à celles déjà mentionnées, telles que la durée de conservation des données dans le cloud, le fondement juridique pour le transfert dans le cloud, le type de données déversé dans le cloud, ou bien les droits pour la personne concernée dans le cloud (etc.).

On remarquera que l'art. 19, nLPD, n'exige pas de forme spécifique pour la communication des informations. En pratique une déclaration de protection des données, mise à disposition de la personne concernée, est souvent la forme privilégiée [52]. Il est encore intéressant de noter que l'art. 19, nLPD, n'impose pas la notification des modifications intervenant postérieurement à la collecte de données (comme le changement des pays dans lesquels opèrent les datacenters cloud, ou la sous-traitance par de nouveaux prestaires cloud, etc) à la personne concernée [53]. Seul l'état au moment de la collecte est censé faire l'objet d'une communication informationnelle par le responsable du traitement.

Des exceptions au devoir d'informer sont listées à l'article 20, nLPD. En particulier, le responsable est délié de son devoir d'informer si la personne concernée est déjà en possession de l'information ou si le traitement de données est prévu par une base légale (art. 20, al. 1, let. a et b, nLPD). En vertu de ce dernier point, la quasi-totalité des traitements de données effectués par les organes fédéraux ne requièrent pas l'information de la personne concernée, puisqu'ils se fondent en principe sur une base légale (art. 34, al. 1, 2 et 3, nLPD). David Rosenthal (2020) qualifie cet état de fait, bénéficiant aux organes fédéraux, de surprenant et de probable oubli du législateur [54]. Le devoir d'information ne s'applique pas non plus s'il nécessite des efforts disproportionnés pour le responsable du traitement (art. 20, al. 2, let. b, nLPD).

[51] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p. 40.
[52] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p. 41.
[53] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p. 39.
[54] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p. 38 et 42.

ÉTAPE 6 : le responsable du traitement, recourant à un service cloud externe, informe-t-il la personne concernée de manière conforme à la nLPD ?

- ⇨ **6.1)** lors du recours à un service cloud externe pour le traitement de ses données, la personne concernée est-elle informée de la présence de sous-traitants (prestaires de clouds) dans la chaîne de traitement (art. 19, al. 2, let. c, nLPD) ?
- ⇨ **6.2)** dans le cas où des données sont communiquées sur des clouds à l'étranger, la personne concernée est-elle informée de la zone de destination ainsi que de son adéquation en matière de protection des données (art. 19, al. 4, nLPD) ? En particulier, si le niveau de protection des données des pays de destination n'est pas adéquat, la personne concernée est-elle informée des garanties prévues au sens de l'art. 16, al. 2, nLPD, ou des exceptions appliquées au sens de l'art. 17, nLPD ?
- ⇨ **6.3)** dans le cas où les circonstances imposent au responsable de communiquer à la personne concernée certains éléments afin qu'elle fasse valoir ses droits au sens de la nLPD, et que la transparence du traitement dans le cloud puisse être garantie (art. 19, al. 2, nLPD), ces éléments sont-ils effectivement communiqués ?
- ⇨ **6.4)** si le responsable du traitement n'accorde pas les éléments informationnels prescrits à l'article 19, nLPD, le cas se rapporte-il aux exceptions et restrictions prévues à l'article 20, nLPD ?

Si 4x OUI, la personne concernée est correctement informée , par le responsable, du traitement de ses données dans le cloud, au sens de la nLPD

Si 1x NON, le responsable n'informe pas la personne concernée du traitement de ses données dans le cloud de manière conforme à la nLPD

Le responsable du traitement agit comme une personne privée :

- ➢ les personnes privées, responsables du traitement, qui, par dol, contreviennent aux obligations prévues à l'article 19 en fournissant des renseignements inexacts ou incomplets, ou omettent d'informer la personne concernée conformément à l'article 19, al. 1, ou encore ne fournissent pas les informations prévues à l'article 19, al. 2, s'exposent, sur plainte de la personne concernée, à une amende de 250'000 francs (conformément à l'art. 60, al. 1, let. a et let. b, ch. 1 et 2, nLPD).
- ➢ une action en responsabilité civile du responsable du traitement est réservée en cas d'atteinte illicite ayant fautivement causé un dommage à la personne concernée (art. 41, CO).

Le responsable du traitement est un organe fédéral, agissant comme une personne publique :

- ➢ si le traitement dans le cloud est illicite (viole notamment l'art. 19, nLPD), quiconque ayant un intérêt digne de protection peut engager une action au sens de l'article 41, nLPD.

3.7. Droits de la personne concernée (art. 25ss, nLPD)

Le devoir d'informer, énoncé à l'article 19, nLPD, est complété à l'article 25, nLPD, par un droit d'accès à l'information et aux données pour la personne concernée. Fondamentalement, ce droit d'accès n'octroie pas à la personne concernée la possibilité d'obtenir de nombreux éléments supplémentaires en lien avec une externalisation du traitement de ses données sur le cloud. Il est cependant intéressant de noter deux facultés additionnelles apportées par l'article 25, nLPD, en comparaison à l'article 19, nLPD.

Premièrement, le droit d'accès n'est pas limité à la collecte de données, contrairement au devoir d'informer. Ainsi, la personne concernée peut exercer son droit d'accès en cours de traitement et être avisée de l'évolution de l'ensemble des informations utiles à la défense de ses droits et nécessaires à la transparence de son traitement (art. 25, al. 2, nLPD). Typiquement, elle peut obtenir des informations relatives à de nouveaux acteurs impliqués dans la chaîne de traitement (identité de nouveaux prestataires cloud ou alors recours à une catégorie de sous-traitants), ainsi qu'à de nouveaux Etats de destination pour la communication des données (désignation des nouveaux Etats, appréciation de leur niveau de protection des données, ainsi que les mesures de garanties entreprises le cas échéant) (art. 25, al. 2, let. g, nLPD). Ces informations doivent en principe être communiquées par le responsable du traitement dans un délai de 30 jours suivant la requête d'accès de la personne concernée (art. 25, al. 7, nLPD).

Deuxièmement, en vertu de l'art. 25, al. 2, let. d, nLPD, le responsable d'un traitement est obligé de communiquer la durée de conservation des données (dans le cloud si elles y sont stockées) si la personne concernée le demande. En ce sens, l'article 25, nLPD, s'avère plus exigeant que l'article 19, nLPD, qui requiert que ces informations ne soient livrées par le responsable du traitement que lorsque les circonstances le suggèrent. Néanmoins, il faut relever que le droit d'accès n'est pas absolu et ne saurait correspondre à un droit d'audit dissimulé pour les personnes concernées [55]. En effet, de nombreuses restrictions au droit d'accès sont énumérées aux articles 26 et 27, nLPD.

Finalement, l'article 28, nLPD, consacre un droit à la remise ou à la transmission des données pour la personne concernée. Ce droit peut être exercé pour autant que certaines conditions soient remplies, comme un traitement légitimé par le consentement de la personne concernée (art. 28, al. 1, let. b, nLPD). Ainsi, à la demande de la personne concernée, le responsable du traitement doit lui remettre, sous un format électronique courant, les données personnelles qu'elle traite à son endroit. La personne concernée peut également exiger du responsable du traitement qu'il transmette directement les données à un autre responsable de traitement (art. 28, al. 2, nLPD). Ce droit à la remise ou à la transmission des données pose des problématiques évidentes pour le responsable du traitement en cas d'externalisation de ses fonctions informatiques sur le cloud. En effet, un nombre important de clouds présentent des technologies, des formats de données ou encore des interfaces non-standardisées. Préalablement au déversement des données sur le cloud, le responsable du traitement doit donc s'assurer de la possibilité effective du rapatriement, de la portabilité et de l'interopérabilité des données évoluant dans le cloud. Comme mentionné à de multiples reprises, le responsable du traitement doit aussi s'assurer qu'il possède en tout temps la maîtrise sur les données qu'il a lui-même déportées sur le cloud.

ÉTAPE 7 : la personne concernée peut-elle jouir de ses droits de manière conforme à la nLPD ?

- ⇨ **7.1)** la personne concernée peut-elle exercer son droit d'accès de manière conforme à la nLPD (art. 25ss, nLPD) ? En particulier, peut-elle obtenir, en tout instant du traitement, les catégories ou l'identité des prestataires clouds sous-traitant ses données (art. 25, al. 2, let. g, nLPD) ? Peut-elle également obtenir les informations relatives à la durée de conservation de ses données dans le cloud ou celles relatives à la communication transfrontalière de ses données vers le cloud (art. 25, al. 2, let. d et g, nLPD) ? De manière plus large, a-t-elle accès à l'ensemble des informations lui permettant de faire valoir ses droits au sens de la nLPD et garantissant la transparence de son traitement (art. 25, al. 2, nLPD) ?
- ⇨ **7.2)** si le responsable du traitement n'accorde pas les éléments informationnels prescrits à l'article 25, nLPD, le cas se rapporte-il aux restrictions prévues aux articles 26 et 27, nLPD ?
- ⇨ **7.3)** la personne concernée peut-elle jouir de son droit à la remise ou à la transmission des données de manière conforme à la nLPD, au regard des conditions posées à l'article 28, al. 1, let. a et b, nLPD ? En particulier, le responsable du traitement s'est-il assuré de la possibilité effective d'un rapatriement, d'une portabilité et de l'interopérabilité des données qu'il a déversées dans le cloud ?
- ⇨ **7.4)** si le responsable du traitement refuse, restreint ou diffère la remise ou la transmission des données, le cas se rapporte-il aux restrictions prévues à l'art. 29, al. 1, nLPD ?

Si 4x OUI, la personne concernée peut jouir de ses droits de manière conforme à la nLPD

Si 1x NON, la personne concernée est empêchée dans l'exercice de ses droits, couverts par la nLPD

Le responsable du traitement agit comme une personne privée :

- ➢ les personnes privées, responsables du traitement, qui, par dol, contreviennent aux obligations prévues à l'article 25ss en fournissant des renseignements inexacts ou incomplets, s'exposent, sur plainte de la personne concernée, à une amende de 250'000 francs
- ➢ une action en responsabilité civile du responsable du traitement est réservée en cas d'atteinte illicite ayant fautivement causé un dommage à la personne concernée (art. 41, CO).

Le responsable du traitement est un organe fédéral, agissant comme une personne publique :

- ➢ si le traitement dans le cloud est illicite (viole notamment les articles 25ss et 28ss, nLPD), quiconque ayant un intérêt digne de protection peut engager une action au sens de l'article 41, nLPD.

[55] ROSENTHAL, David et STUDER, Samira / LOMBARD, Alexandre (pour la traduction), 2020, p. 48.

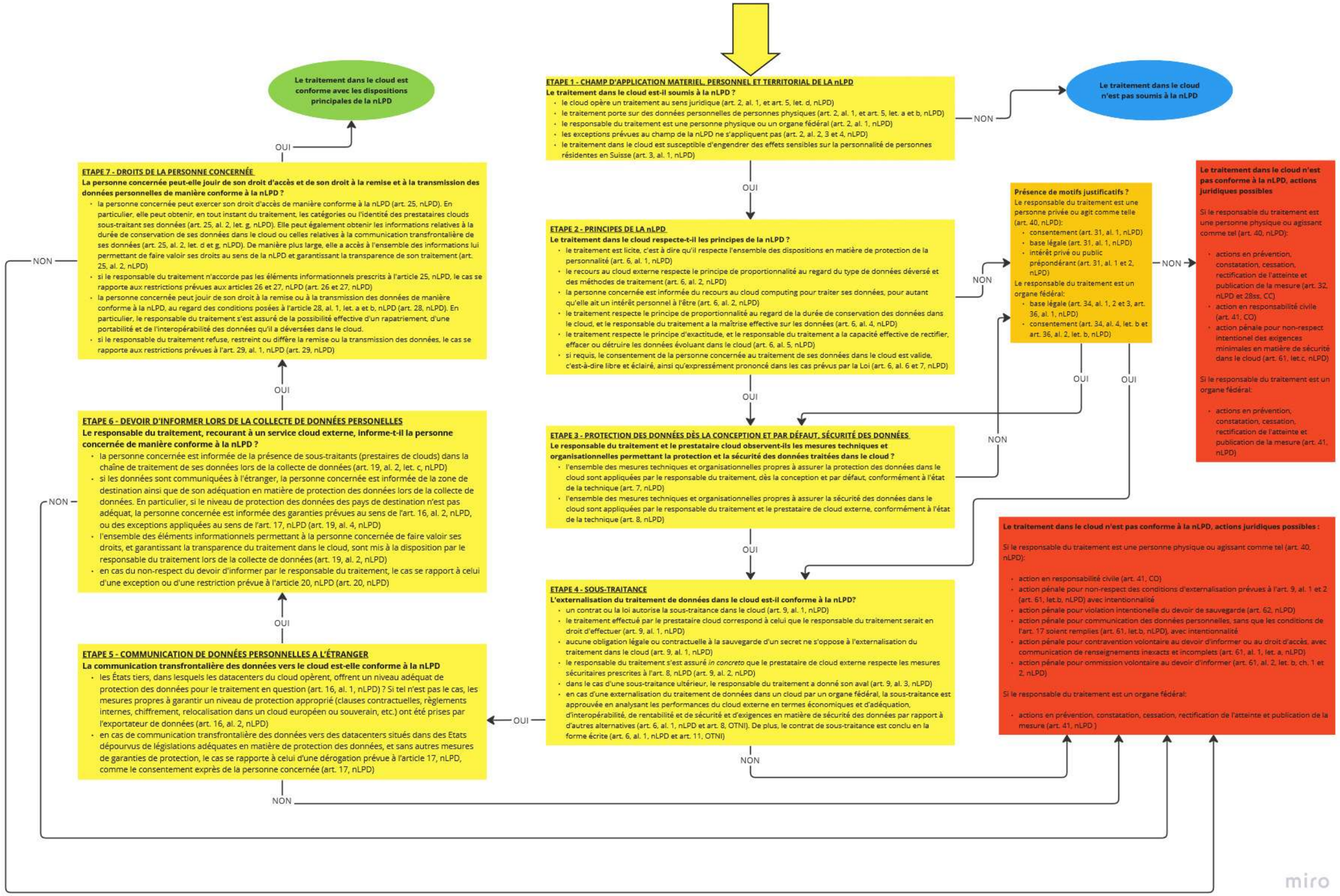

Figure n°2 : logigramme décisionnel simplifié permettant d'apprécier la conformité à la nLPD du recours à un cloud externe par le responsable d'un traitement

4. Casus : le projet de cloud computing "Public Clouds Confederation" est-t-il compatible avec le droit suisse en matière de protection des données pour les personnes physiques ?

Ce casus porte sur l'étude de la compatibilité du projet de cloud public fédéral "Public Clouds Confederation" avec le droit suisse en matière de protection des données.

4.1. Historique du projet "Public Clouds Confederation"

La Confédération a adopté sa stratégie d'informatique en nuage (SB020) lors de sa séance du 11 décembre 2020. Cette dernière est mise en œuvre depuis le 1er janvier 2021. Elle a pour but de faciliter l'utilisation des services cloud par l'administration fédérale [56].

La stratégie d'informatique en nuage de la Confédération (SB020) a notamment introduit le cloud public comme une nouvelle option en matière d'approvisionnement informatique. Le recours sécurisé, performant et structuré au cloud public devrait permettre l'accès aux technologies les plus récentes. La population et les entreprises suisses bénéficieraient ainsi de services administratifs rentables et innovants. Quant aux départements fédéraux et à la Chancellerie fédérale, ils pourraient pallier leurs besoins urgents en hébergement et en capacité de traitement. Le cloud public ne serait qu'un élément de plus de l'architecture informatique de l'administration fédérale, et viendrait se greffer à un écosystème complet, composé de divers modèles d'approvisionnement (services gérés en interne, clouds privés, hybrides, publics, communautaires, multi-clouds, services gérés en externe (voir figure n°3)) [56].

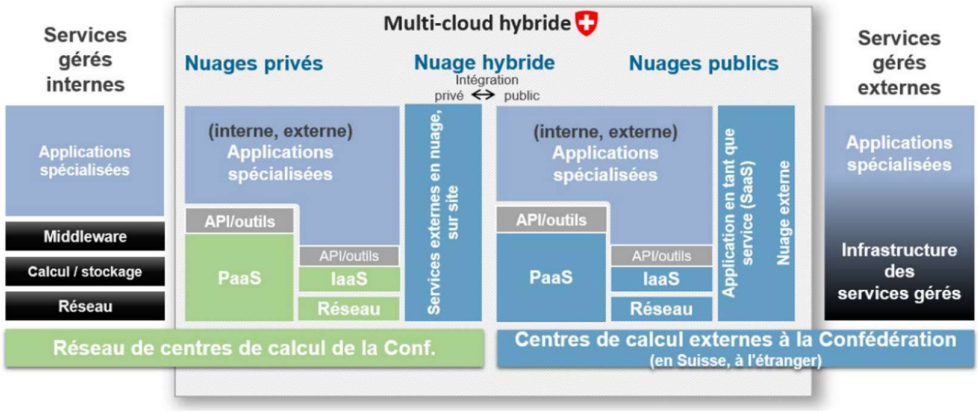

Figure n°3 : Modèle cible de l'informatique en nuage de l'administration fédérale à l'horizon 2025, légende et image extraites du rapport du Conseil fédéral au sujet de la Stratégie d'informatique en nuage de l'administration fédérale, décembre 2020 [56]

Dans la SB020, l'option d'un cloud étatique, nommé "Swiss Cloud", a été envisagée pour couvrir l'ensemble des besoins en cloud public de l'administration fédérale. Le "Swiss Cloud" aurait pris la forme d'une infrastructure indépendante, de droit public. Le 6 avril 2020, le Conseil fédéral a requis un rapport de faisabilité au sujet du développement d'un "Swiss Cloud". En décembre 2020, le rapport sur l'évaluation des besoins d'un nuage informatique suisse n'est pas parvenu à démontrer la nécessité de ce dernier [57].

Par la suite, un examen supplémentaire a été commandé par la Confédération pour déterminer l'utilité de développer un système de certification étatique pour les services cloud. L'examen a conclu qu'une règlementation publique n'était pas nécessaire. Finalement, des travaux ont été menés pour apprécier

[56] Conseil fédéral, *Stratégie d'informatique en nuage de l'administration fédérale*, 2020, p.5-6.
[57] Département fédéral des finances DFF, Unité de pilotage informatique de la Confédération UPIC, *Rapport sur l'évaluation des besoins d'un nuage informatique suisse («Swiss Cloud»)*, 2020, p.4 et p.30.

l'opportunité de rejoindre des initiatives européennes de clouds publics, comme GAIA-X [58]. Les résultats ne semblent pas avoir été fructueux, mais aucune information additionnelle n'a été trouvée à ce sujet.

Le 7 décembre 2020, la Confédération s'est résolue à publier un appel d'offres (OMC-20007) en vue de sélectionner les futurs fournisseurs du cloud public. C'est le lancement du projet "Public Clouds Confederation". L'appel d'offres a prévu la sous-traitance du cloud public fédéral à un consortium d'au maximum cinq prestataires privés. Le délai pour le dépôt des offres a été fixé au 3 février 2021 [59]. Etonnamment, l'appel d'offres élimine *de facto* les potentiels prestataires suisses ou européens. En effet, le cahier des charges de l'OMC-20007 exige que le soumissionnaire gère des datacenters sur trois continents différents et possède une clientèle internationale (point 3.8) [59]. A ce titre, Swisscom, ELCA, Proton, Infomaniak, entreprises 100% helvétiques, renoncent à participer ou critiquent les charges de l'appel d'offres [60, 61, 62]. Parallèlement, durant la phase d'élaboration des offres, les quelques acteurs locaux qui sont potentiellement intéressés au marché "Public Clouds Confederation" peinent à échanger avec la Confédération. Finalement, l'ensemble des exigences posées par le cahier des charges apparaît dantesque et le délai de deux mois est tout simplement impossible à tenir pour les moyennes entreprises. Ainsi, Infomaniak annonce qu'elle devrait mobiliser des équipes à temps plein, des semaines durant, ne serait-ce que pour pouvoir remplir le formulaire de candidature [63].

Le 14 juin 2021, le marché "Public Clouds Confederation" est finalement adjugé à cinq entreprises, dont quatre américaines (Amazon, IBM, Microsoft, Oracle) et une chinoise (Alibaba). La raison de l'attribution du marché est essentiellement justifiée par le prix attractif et les rabais offerts. La Confédération devra ainsi verser à ces entreprises 110 millions de francs suisses de septembre 2021 à août 2026 [64]. L'adjudication à cinq entreprises extra-européennes, dont les sièges se situent dans des pays avec des niveaux de protection des données jugés inadéquats par le Conseil fédéral lui-même, crée de l'incompréhension, de l'inquiétude, voire de la colère chez de nombreux professeurs et juristes, spécialisés en protection des données et cybersécurité, ainsi que chez les entreprises informatiques suisses. Il semble en effet bien loin le temps où la Confédération plébiscitait l'émergence d'une souveraineté numérique et encourageait le développement de la capacité stratégique locale.

Le 13 juillet 2021, Google, une des trois candidatures malheureuses, a fait recours auprès du TAF. Elle a jugé que sa solution cloud satisfaisait au mieux le cahier des charges de l'appel d'offres. De plus, Google a critiqué le cahier des charges sur son manque de clarté concernant les plans de géo-redondances réclamés aux soumissionnaires, critère sur lequel Google a obtenu zéro point. Le 18 octobre 2021, le TAF a rejeté le recours de Google [65]. Le 18 janvier 2022, c'est au tour d'un particulier de saisir le TAF en vue d'invalider le projet "Public Clouds Confederation" qui recourt à des fournisseurs étrangers. L'intéressé réclame notamment des mesures provisionnelles. Le 27 octobre 2022, le TAF a rejeté sa requête au motif de l'absence d'un risque concret et imminent de transfert de données du requérant [66].

Le 27 septembre 2022, l'annonce est faite par la Confédération de la signature des contrats cloud avec les cinq fournisseurs étrangers [67]. Les contrats, n'ont, à ce jour, toujours pas été rendus publics. Dès le 2 novembre 2022, le Conseil fédéral autorise les unités administratives à acheter des services cloud dans le cadre du "Public Clouds Confederation". Elles doivent cependant observer les prescriptions en matière de protection des données et de sécurité de l'information lors du recours à ces services. Préalablement à l'achat de services cloud, une unité

[58] Chancellerie fédérale, ChF, *Swiss Cloud*, 2021.
[59] simap.ch, nº de publication 1136861.
[60] RTSinfo, *Google recourt contre le choix des fournisseurs pour le "cloud" de la Confédération*, 2021.
[61] RTS, *La Suisse sous Couverture*, 2022.
[62] Le Temps, *Les partisans d'un cloud suisse contre-attaquent et ciblent le Conseil fédéral*, 2021.
[63] infomaniaknews, *La Suisse renonce à la notion de souveraineté numérique et cède aux entreprises américaines et chinoises*, 2021.
[64] Le Temps, *Surprise, la Confédération se fournit en Chine pour son cloud*, 2021.
[65] ATAF 2021 IV/6
[66] ATAF-661/2022
[67] Conseil fédéral, portail du Gouvernement suisse, *Les contrats du projet « Public Clouds Confédération » sont signés*, 2022.

administrative fédérale doit ainsi établir un cahier des charges indépendant et clarifier les enjeux de sécurité et les risques pour la protection des données déportées [68, 69]. Les principes qui devront être respectés lors de l'achat de services cloud par une unité administrative sont en cours d'élaboration par le secteur TNI de la Chancellerie fédérale, qui gouverne le cloud public. Ils seront à priori communiqués au deuxième semestre 2023. Par ailleurs, les organes fédéraux pourront bénéficier des conseils du Cloud Service Broker (CSB), rattaché à l'Office fédéral de l'informatique et de la télécommunication (OFIT), lors d'un recours au "Public Clouds Confederation" [70].

4.2. Conformité du projet "Public Clouds Confederation" avec la nLPD

En l'absence d'informations précises quant au contenu des contrats signés et de la nature des données transférées dans le cadre du "Public Clouds Confederation", la question de la conformité du projet à la nLPD va se poser ici uniquement à l'égard du droit de sous-traitance et du principe de proportionnalité. En effet, en raison du peu d'informations disponibles, il n'est pas possible d'apprécier la conformité du projet "Public Clouds Confederation" à l'égard de l'ensemble des principales dispositions de la nLPD, tel que proposé au chapitre 3.

Comme évoqué aux pages 13 et 14, un organe fédéral est autorisé à sous-traiter les données personnelles qu'il détient dans le cloud pour autant que des bases légales le prévoient (art. 9, al. 1, nLPD). C'est le cas de l'article 8, OTNI, qui autorise l'externalisation des fonctions informatiques par des unités administratives pour autant que la décision soit motivée par des analyses de marché et des principes d'adéquation, d'interopérabilité, de rentabilité et des exigences en matière de sécurité. Ainsi, au sens de l'article 8, OTNI, le "Public Cloud Confederation", géré par des entreprises étrangères, serait une solution proportionnée s'il présentait des avantages technologiques et financiers significatifs pour la Suisse par rapport aux autres alternatives analysées (cloud interne ou "Swiss Cloud") tout en permettant une protection des données raisonnables pour les résidents suisses dont les données sont traitées. Or, dans le cas d'espèce, il est fâcheux de constater que non seulement la protection de la personnalité et la sécurité des données ne bénéficient pas de l'option choisie (c'est-à-dire du cloud public fourni par Amazon, IBM, Microsoft, Oracle et Alibaba), mais que les avantages en termes financiers et technologiques sont également discutables.

Premièrement, en ce qui concerne la protection de la personnalité des personnes dont les données sont traitées, les pays de destination du cloud ne sont pas réputés pour être des chantres en matière de protection des données. En effet, Amazon, IBM, Microsoft et Oracle sont des entreprises américaines, soumises au *CLOUD Act* depuis 2018 (cf. page 7). Elles sont par conséquent contraintes de communiquer des données situées dans le cloud sous simple requête des autorités américaines, peu importe le lieu des datacenters de traitement. Du côté d'Alibaba, ce n'est guère plus réjouissant, puisque la Chine a promulgué la Loi sur la cybersécurité (LCS) le 7 novembre 2016, obligeant ses entreprises à collaborer sans limites et en toute discrétion sur demande des services de renseignement nationaux [71, 72]. De plus, Solange Ghernaouti, professeure en cybersécurité et cyberdéfense à l'Université de Lausanne, insiste aussi sur la forte asymétrie de pouvoir qui règne entre les cinq fournisseurs de services et la Confédération. Il n'est pas impossible que les prestataires modifient les règles concernant l'accès aux données, comme ils le souhaitent [71]. Même son de cloche du côté de l'entreprise Infomaniak qui ajoute : "Si toutes les équipes de développement sont à l'étranger, qu'arrivera-t-il en cas de désaccord commercial, juridique ou diplomatique ? La Confédération sait-elle déjà à coup sûr à quelle sauce elle sera mangée ? Même si ces

[68] Conseil fédéral, portail du Gouvernement suisse, *« Public Clouds Confédération » : les prestations peuvent être commandées*, 2022.
[69] Conseil fédéral, portail du Gouvernement suisse, *« Public Clouds Confédération » - préparation des contrats avec les fournisseurs*, 2022.
[70] Chancellerie fédérale, ChF, *Publics Cloud Confederation*, 2022.
[71] RTSinfo, émission FORUM, 2021.
[72] Gouvernement du Canada, portail des PME, 2022.

fournisseurs devaient présenter des certifications, les risques directement liés à l'absence de souveraineté existent bel et bien (…)." [73].

Deuxièmement, en ce qui concerne les aspects financiers, l'entreprise Infomaniak, toujours elle, ironise de manière percutante sur les économies vantées par la Confédération dans le cadre du projet "Public Clouds Confederation". En effet, Infomaniak se demande si le renforcement de l'hégémonie des GAFAM, l'accélération de l'arrivée des BATX sur le marché, le retardement de l'émergence de la souveraineté suisse ou encore le frein au développement de la capacité industrielle stratégique suisse, engendrés par le "Public Clouds Confederation", ont été pris en compte au moment de faire l'addition économique [73]. Ainsi, si le coût direct du cloud public fédéral est de prime abord alléchant, le coût indirect incluant le manque à gagner et le coût d'opportunité pour le tissu économique suisse risque de s'avérer bien moins idyllique à terme. Au passage, d'aucuns pourraient critiquer l'appel d'offres OMC-20007 qui accorde 40% des points aux critères "prix" et "rabais", et seulement 10% à "l'emplacement des centres de données en Suisse" [74]. Il semble légitime de se questionner sur le respect du principe de proportionnalité quant à la balance des différents intérêts en présence (sécuritaires, économiques et stratégiques) réalisée par la Confédération. De plus, François Charlet, spécialiste du droit des technologies, précise que cette balance n'intègre pas des facteurs importants, comme la géopolitique [73].

Troisièmement, en ce qui concerne les avantages techniques, la solution "Public Clouds Confederation" est indéniablement la meilleure à court terme. Aucune entreprise suisse ou européenne n'a, du moins actuellement, les moyens techniques d'offrir à elle seule un cloud public pour la Confédération. Néanmoins, une coalition d'entreprises suisses et européennes aurait dû être en mesure de répondre à certains besoins de l'administration fédérale [75, 76]. Cela aurait encouragé, de manière vertueuse, l'émergence d'une souveraineté numérique suisse et européenne et le développement de compétences et de savoir-faire locaux.

Finalement, au sens de l'art. 8, OTNI, une analyse de marché est ordonnée lors du recours à un service de cloud externe par l'administration fédérale. Or, dans le cas d'espèce, les entreprises suisses et européennes ont été *de facto* exclues du marché par les conditions de l'appel d'offres qui demandaient une présence des datacenters sur trois continents différents. La professeur Solange Ghernaouti énonce à ce sujet qu'il est nécessaire que la proportionnalité entre les exigences fixées par le cahier des charges et les besoins réels à couvrir soit garantie [77]. Or précisément, les besoins du "Public Clouds Confederation" n'ont pas été clairement statués dans l'appel d'offres, et l'exigence d'une présence sur les trois continents ne semble, en l'état, pas justifié.

En l'absence de transparence au sujet du "Public Cloud Confederation", il est difficile d'émettre un avis ferme et définitif sur la conformité de ce projet à la nLPD. Par exemple, si aucune donnée personnelle n'est versée dans le cloud public, la question ne se posera même pas puisque le cloud ne sera pas assujetti à la nLPD (art. 2, al. 1, nLPD). Néanmoins, à la lecture des avis de professeurs, juristes et entreprises spécialisés en matière de protection des données, de forts doutes demeurent quant à la proportionnalité de l'externalisation des fonctions informatiques de l'administration sur des clouds américains et chinois. Des alternatives locales ou européennes auraient sans doute permis d'assurer une meilleure sécurité pour les données transférées, tout en ménageant les composantes économiques et techniques à long terme.

Pour conclure, le principe de proportionnalité de l'article 6, alinéa 2, nLPD et de l'article 8, OTNI, semblent avoir été durement maltraités par la solution apportée par le "Public Clouds Confederation".

---

[73] infomaniaknews, *La Suisse renonce à la notion de souveraineté numérique et cède aux entreprises américaines et chinoises*, 2021.
[74] simap.ch, nº de publication 1136861.
[75] RTS, *La Suisse sous Couverture*, 2022.
[76] Le Temps, *Les partisans d'un cloud suisse contre-attaquent et ciblent le Conseil fédéral*, 2021.
[77] infomaniaknews, *Cybersécurité et souveraineté numérique : réponses aux questions que nous recevons avec Solange Ghernaouti*, 2022.

Bibliographie

HUSSAIN, Zarmine et CHUFFART-FINSTERWALD, Stéphanie, *Exclue du champ de Loi fédérale sur la protection des données : la protection des données des personnes morales* , sigma legal SA, 3 janvier 2023.
Accessible sur :
https://www.sigmalegal.ch/fr/actualites/exclue-du-champ-de-loi-federale-sur-la-protection-des-donnees-la-protection-des-donnees-des-personnes-morales/
(consulté le 7 avril 2023)

Confédération Suisse, portail PME pour petites et moyennes entreprises, *Nouvelle loi sur la protection des données (nLPD)*, 24 novembre 2022.
Accessible sur :
https://www.kmu.admin.ch/kmu/fr/home/faits-et-tendances/digitalisation/protection-des-donnees/nouvelle-loi-sur-la-protection-des-donnees-nlpd.html
(consulté le 7 avril 2023)

Conseil fédéral, portail du Gouvernement suisse, *« Public Clouds Confédération » : les prestations peuvent être commandées*, 2 novembre 2022.
Accessible sur :
https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-91092.html
(consulté le 7 avril 2023)

Gouvernement du Canada, portail des PME, *Le régime chinois de cybersécurité*, 12 octobre 2022.
Accessible sur :
https://www.deleguescommerciaux.gc.ca/china-chine/cyber-security_cyber-securite_china-chine.aspx?lang=fra
(consulté le 7 avril 2023)

Conseil fédéral, portail du Gouvernement suisse, *Les contrats du projet « Public Clouds Confédération » sont signés*, 27 septembre 2022.
Accessible sur :
https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-90509.html
(consulté le 7 avril 2023)

Confédération suisse, Chancellerie fédérale ChF, *Swiss Cloud*, 26 septembre 2022.
Accessible sur :
https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud/public-clouds-bund.html
(consulté le 7 avril 2023

Périodique CANTON-COMMUNES nº64, *Le cloud computing*, 21 juin 2022.
Accessible sur :
https://info.vd.ch/canton-communes/2022/juin/numero-64/le-cloud-computing
(consulté le 7 avril 2023)

Everwin.fr, *Cloud Computing - SaaS, IaaS, et PaaS : Définitions et différences !*, 19 mai 2022.
Accessible sur :
https://everwin.fr/cloud-computing-saas-iaas-paas/
(consulté le 7 avril 2023)

RTS, *La Suisse sous Couverture*, Episode 1, Saison 2, 25 avril 2022.
Accessible sur :
https://www.rts.ch/docs/13032515--la-suisse-sous-couverture-.html
(consulté le 7 avril 2023)

infomaniaknews, *Cybersécurité et souveraineté numérique : réponses aux questions que nous recevons avec Solange Ghernaouti*, 7 mars 2022.
Accessible sur :
https://news.infomaniak.com/cybersecurite-et-souverainete-numerique/
(consulté le 7 avril 2023)

Conseil fédéral, portail du Gouvernement suisse, *« Public Clouds Confédération » – préparation des contrats avec les fournisseurs*, 1er mars 2022.
Accessible sur :
https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-87412.html
(consulté le 7 avril 2023)

Le Temps, *Les partisans d'un cloud suisse contre-attaquent et ciblent le Conseil fédéral*, 9 septembre 2021.
Accessible sur :
https://www.letemps.ch/economie/cyber/partisans-dun-cloud-suisse-contreattaquent-ciblent-conseil-federal
(consulté le 7 avril 2023)

PFPDT, *Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données requis, en application de clauses contractuelles types et de contrats types reconnus 27 août 2021*, 27 août 2021.
Accessible sur :
https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html
(consulté le 7 avril 2023)

RTSinfo, *Google recourt contre le choix des fournisseurs pour le "cloud" de la Confédération*, 21 juillet 2021.
Accessible sur :
https://www.rts.ch/info/suisse/12362324-google-recourt-contre-le-choix-des-fournisseurs-pour-le-cloud-de-la-confederation.html
(consulté le 7 avril 2023)

infomaniaknews, *La Suisse renonce à la notion de souveraineté numérique et cède aux entreprises américaines et chinoises*, 12 juillet 2021.
Accessible sur :
https://news.infomaniak.com/souverainete-numerique-de-la-suisse/
(consulté le 7 avril 2023)

RTSinfo, émission FORUM, *Service cloud, La Confédération choisit le Chinois Alibaba*, 30 juin 2021.
Accessible sur :
https://www.rts.ch/play/tv/forum/video/le-fournisseur-chinois-alibaba-va-stocker-des-donnees-administratives-federales-interview-de-solange-ghernaouti?urn=urn:rts:video:12315747
(consulté le 7 avril 2023)

Le Temps, *Surprise, la Confédération se fournit en Chine pour son cloud*, 28 juin 2021.
Accessible sur :
https://www.letemps.ch/economie/cyber/surprise-confederation-se-fournit-chine-cloud
(consulté le 7 avril 2023)

PFPDT, *Guide pour l'examen de la licéité de la communication transfrontière de données*, 28 juin 2021.
Accessible sur :
https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-629182963
(consulté le 7 avril 2023)

Confédération suisse, Chancellerie fédérale ChF, *Swiss Cloud*, 11 mars 2021.
Accessible sur :
https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud/swiss-cloud.html
(consulté le 7 avril 2023)

METILLE, Sylvain, *Le traitement de données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020*, Semaine Judiciaire 2021 II, mars 2021.
Accessible sur :
https://serval.unil.ch/resource/serval:BIB_50B41488B453.P001/REF
(consulté le 7 avril 2023)

Conseil fédéral, portail du gouvernement suisse, *Stratégie d'informatique en nuage de l'administration fédérale*, 11 décembre 2020.
Accessible sur :
https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-81568.html
(consulté le 7 avril 2023)

Département fédéral des finances DFF, Unité de pilotage informatique de la Confédération UPIC, *Rapport sur l'évaluation des besoins d'un nuage informatique suisse («Swiss Cloud»)*, décembre 2020.
Accessible sur :
https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud/swiss-cloud.html
(consulté le 7 avril 2023)

ROSENTHAL, David et pour la traduction : STUDER Samira / LOMBARD, Alexandre, *La nouvelle loi sur la protection des données*, Jusletter, 16 novembre 2020.
Accessible sur :
https://www.rosenthal.ch/downloads/Rosenthal-Studer-Lombard-nouvelleLPD.pdf
(consulté le 7 avril 2023)

PFPDT, *Prise de position sur la transmission de données personnelles vers les États-Unis et d'autres États n'offrant pas un niveau adéquat de protection des données au sens de l'art. 6, al.1 LPD*, 8 septembre 2020.
Accessible sur :
https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html
(consulté le 7 avril 2023)

METILLE, Sylvain, *L'utilisation de l'informatique en nuage par l'administration publique*, AJP/PJA 6/2019, juin 2019.
Accessible sur :
https://serval.unil.ch/resource/serval:BIB_F35D8E36D365.P001/REF
(consulté le 7 avril 2023)

RUFENER, Adrian, *"Clic informatique" : travailler dans le cloud*, Anwaltsrevue, 6/7/2013, juillet 2013.
Accessible sur :
https://anwaltsrevue.recht.ch/de/artikel/11arv0613prx/clic-informatique-travailler-dans-le-cloud
(consulté le 7 avril 2023)

FANTI, Sébastien, *Cloud computing : opportunités et risques pour les avocats*, Anwaltsrevue, 2/2013, février 2013.
Accessible sur :
https://anwaltsrevue.recht.ch/fr/artikel/02arv0213prx/cloud-computing-opportunites-et-risques-pour-les-avocats
(consulté le 7 avril 2023)

MELL, Peter et GRANCE, Timothy, *The NIST Definition of Cloud Computing, National Institute of Standards and Technology*, NIST, U.S. Department of Commerce, Special Publication 800-145, Gaithersburg, 2011.
Accessible sur :
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
(consulté le 7 avril 2023)

MEIER, Philippe, *Protection des données – Fondements, principes généraux et droit privé*, Berne 2011.

PFPDT, *Explications concernant l'informatique en nuage (cloud computing)*, 2011.
Accessible sur :
https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html
(consulté le 7 avril 2023)