Berne, le 31 août 2022

Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale

Rapport en exécution du jalon 5 de la stratégie d'informatique en nuage du Conseil fédéral

Liste des modifications

Version	Date	Modification	Nom
0.1		Projet pour la 1re séance du groupe de travail[1]	Ronja Lichtsteiner / Stephan Brunner
0.2	21.1.2022	Révision, projet pour la 2e séance du groupe de travail	Ronja Lichtsteiner / Stephan Brunner
0.3		Révision après la 2e réunion du groupe de travail, intégration remarques OFJ	Ronja Lichtsteiner / Stephan Brunner
0.4	04.03.2022	Révision, intégration remarques PFPDT	Ronja Lichtsteiner
0.5	08.03.2022	Révision, intégration remarques LauxLawyers AG	Ronja Lichtsteiner / Stephan Brunner
0.6	09.03.2022	Révision, intégration remarques TNI	Ronja Lichtsteiner / Stephan Brunner
0.7	18.03.2022	Révision après passage à la direction ChF	Ronja Lichtsteiner / Stephan Brunner
0.8	20.06.2022	Révision après CTNI	Ronja Lichtsteiner / Stephan Brunner
1.0	16.08.2022	Révision après consultation des offices	Ronja Lichtsteiner / Stephan Brunner
1.1	31.08.2022	Mise au point rédactionnelle après que la CSG a pris acte du projet	Ronja Lichtsteiner / Stephan Brunner

[1] Les personnes suivantes sont représentées dans le groupe de travail : Stephan Brunner ChF (direction) ; Ronja Lichtsteiner ChF ; Sandra Husi/ Stephanie Schneiter SG-DFJP ; Monique Cossali Sauvain OFJ ; Monica Ratte SG-DFJ ; Melanie Koller SG-DDPS ; représentants du PFPDT ; Angelika Spiess SG-DFJP ; Christian Bachofen SG-DETEC ; Boris Inderbitzin DFAE ; Thomas Fischer, Office d'informatique et d'organisation du canton de Berne

Table des matières

Annexes :

Annexe A : Bibliographie et matériel
Annexe B : Glossaire
Annexe C : Risques et mesures
Annexe D : Liste de contrôle
Annexe E: Vue d'ensemble de l'utilisation de l'informatique en nuage dans l'administration fédérale (Exemples de bonnes pratiques (modèles de déploiement de nuages informatiques)

Synthèse

But du rapport

Le présent rapport doit d'une part clarifier des questions juridiques fondamentales pour l'approvisionnement infonuagique et créer ainsi une compréhension juridique uniforme pour l'administration fédérale. D'autre part, il doit montrer quels sont les moyens disponibles pour évaluer l'admissibilité des projets d'approvisionnement infonuagique et pour garantir leur « conformité ». Il doit pouvoir servir de base, entre autres, à l'analyse des bases juridiques[2] pour les projets d'approvisionnement infonuagique.

Aspects liés aux risques (cf. partie 1 Aspects liés aux risques**)**

Outre le fait que l'unité administrative compétente n'a plus elle-même le contrôle physique des moyens informatiques, trois facteurs en particulier contribuent à la complexité juridique, et technique, des solutions d'approvisionnement infonuagique, ce dont il faut tenir compte lors de l'évaluation des risques (voir annexes C à E) :

- Lien avec l'étranger : à l'heure actuelle, les services issus de nuages publics des grands fournisseurs (fournisseurs hyperscalaires), en particulier, sont potentiellement fournis en tout ou partie à l'étranger (emplacements des serveurs, accès au support). La tendance à la diminution du contrôle sur l'environnement juridique (par ex. en ce qui concerne l'adéquation de la législation sur la protection des données dans le pays de destination et le risque d'accès par les autorités) doit donc être compensée par des mesures contractuelles, techniques et organisationnelles.
- Recours à des sous-traitants : pour l'exécution du mandat, les fournisseurs de services nuagiques (également pour les solutions de nuage privé) font généralement appel à d'autres tiers qui accomplissent certaines tâches. Par ailleurs, ces sous-traitants exécutent parfois leurs tâches à partir de pays tiers.
- Dépendance vis-à-vis de tiers : les solutions d'approvisionnement infonuagique peuvent entraîner une dépendance importante vis-à-vis de certains fournisseurs de services, notamment en ce qui concerne la disponibilité des services.

Décider quels sont les risques résiduels acceptables, dans les limites du droit applicable, est une question de conduite qui relève des responsables du projet. Cette décision doit être prise en fonction de la nature des données à transférer[3] sur la base d'une analyse du cadre juridique et des risques approfondie. L'analyse des risques doit tenir compte des facteurs de risque existants dans le cas d'application concret et des mesures prises pour les atténuer.

Principaux résultats de l'analyse par domaine juridique

*Protection des données (*cf. partie 2 Législation fédérale sur la protection des données*)*

La législation sur la protection des données autorise le sous-traitement de données par des tiers externes à l'administration, sur la base d'un contrat. Si le mandataire recourt à des sous-traitants, le mandant doit garantir par des clauses contractuelles et le cas échéant par des mesures techniques que ceux-ci respectent les mêmes règles que les fournisseurs de services nuagiques (cf. partie 2, ch. 1.5.1).

La loi sur la protection des données prévoit un régime différencié pour la communication de données personnelles à l'étranger. Cette communication est d'autant plus facile que la législation du pays de destination garantit une protection des données équivalente à celle de la Suisse. C'est notamment le cas dans l'UE et au Royaume-Uni.

En ce qui concerne la possibilité pour les autorités étrangères d'accéder à des données se trouvant à l'étranger ou sous le contrôle de mandataires étrangers, il convient de procéder à un examen approfondi dans le cadre de chaque projet. En effet, les autorités de l'État concerné pourraient demander l'accès aux données à l'insu de l'utilisateur de l'informatique en nuage ou y avoir accès sans que l'utilisateur ait la possibilité de s'y opposer par des moyens juridiques. Dans ce contexte, il convient de se demander, en particulier pour les fournisseurs soumis aux lois américaines telles que le CLOUD Act et

[2] Un modèle d'analyse des bases légales se trouve ici : Analyse des bases légales (admin.ch)
[3] Lorsqu'une différenciation n'est pas nécessaire en vertu de la loi, les données et les informations sont utilisées comme synonymes.

la section 702 FISA, si le système juridique du pays dans lequel le service est fourni présente généralement des risques particuliers. Pour le droit américain, on peut partir du principe suivant : les données des autorités suisses bénéficient d'une certaine protection contre l'accès par les autorités américaines, compte tenu des mécanismes procéduraux prévus par le CLOUD Act ; en particulier, il appert que les données des autorités bénéficient d'une protection plus élevée que les données privées (même s'il n'est pas garanti que les autorités américaines ne touchent jamais aux données des autorités suisses). Le risque d'accès - non conforme au droit du point de vue suisse - sur la base du Foreign Intelligence Surveillance Act (FISA) et de l'Executive Order (E.O.) 12.333 peut également être réduit à un niveau juridiquement acceptable si les mécanismes déjà prévus par le droit américain sont complétés contractuellement (en particulier l'obligation de contester une remise) et des mesures de protection techniques.

Un examen doit cependant toujours être effectué au cas par cas et doit éventuellement inclure les risques politiques ; cela vaut également pour les solutions nuagiques impliquant des États de l'UE ou d'autres États tiers (cf. partie 2, ch. 1.6 et annexe C).

Dans la mesure où il s'agit du traitement de données personnelles, il convient de souligner qu'une évaluation différenciée d'un projet concret d'approvisionnement infonuagique est nécessaire. On tiendra compte du type de données concernées et de la manière dont elles sont traitées. En fonction de cela, il est possible d'évaluer si l'externalisation des données dans le nuage est licite et de définir les exigences relatives aux mesures organisationnelles et techniques de protection des données.

Secret de fonction (cf. partie 2 Secret de fonction*)*

Les fournisseurs de services nuagiques sont inclus dans le cercle des dépositaires du secret de fonction en tant qu'auxiliaires dans le nouvel art. 320, ch. 1, du code pénal (RS 311.0 [CP][4]). Il est possible de prendre des mesures techniques (et de les garantir par contrat) pour empêcher dans une large mesure un accès illicite, y compris par le fournisseur de services nuagiques, notamment par le cryptage ou la pseudonymisation et la tokenisation des données (cf. partie 2, ch. 0).

Sont secrets tous les faits qui ne sont ni de notoriété publique, ni généralement accessibles (secret relatif), pour lesquels il existe un intérêt légitime au maintien du secret et que le détenteur du secret veut garder confidentiels (secret matériel ; par exemple informations soumises au secret professionnel conformément à l'art. 321 CP, dispositions sur le secret fiscal, le secret des assurances sociales ou informations correctement classifiées). Le secret de fonction est violé lorsque le détenteur du secret de fonction rend accessibles ces informations à un tiers auquel elles ne sont pas destinées.

Depuis que le principe de transparence a été mis en oeuvre dans l'administration fédérale, le cercle des informations qui sont (ou peuvent être) soumises au secret de fonction s'est réduit. Les informations devenues accessibles en vertu de la loi sur la transparence (RS *152.3*) ou qui peuvent être rendues accessibles en vertu de celle-ci sans restriction ne sont plus soumises au secret de fonction. Les règles de la loi sur la protection des données (RS *235.1*) s'appliquent aux données personnelles et priment les autres dispositions).

Une violation du secret de fonction est donc possible en premier lieu lorsque le fournisseur de services nuagiques (soumis contractuellement au secret de fonction) met à la disposition d'un tiers non autorisé des données couvertes par le secret de fonction. Pour ce faire, le fournisseur de services nuagiques devrait généralement contourner des mesures techniques et violerait donc ses obligations contractuelles et, le cas échéant, des dispositions pénales.

Protection des informations (cf. partie 2 Dispositions concernant la protection des informations*)*

Les règles actuelles ou futures en matière de protection des informations ne s'opposent pas *a priori* à l'approvisionnement infonuagique. Les données jusqu'à l'échelon de classification CONFIDENTIEL inclus peuvent en principe être traitées par les mandataires si des mesures adéquates de protection des informations sont prises. L'adéquation des mesures dépend notamment de la sensibilité des données et du risque d'abus ainsi que du dommage potentiel en cas d'utilisation abusive des données.

L'annexe D *(Liste de contrôle*) donne une vue d'ensemble des questions à clarifier dans l'optique d'une externalisation dans le nuage et des principaux risques à évaluer.

[4] Entrée en vigueur prévue : 1er janvier 2023

Partie 1 – Remarques préliminaires

1 Introduction

1.1 Objet et cercle des destinataires

Le 11 décembre 2020, le Conseil fédéral a adopté la stratégie d'informatique en nuage de l'administration fédérale[5] (EXEBRC 2020.2726), qui vise à faciliter l'utilisation des services en nuage dans l'administration fédérale[6]. Des objectifs et des jalons ont été fixés à cette fin. Le présent rapport met en œuvre une partie du jalon 5 de la stratégie d'informatique en nuage de la Confédération, qui prévoit notamment ce qui suit[7]:

«Clarté juridique (sous la forme d'un rapport) concernant les dispositions des normes légales pertinentes et les règles internes à l'administration qui portent sur l'utilisation de services en nuage public. Cela englobe notamment les lois et ordonnances suisses (par ex. LMSI, LPers, OPDC, OCSP, LOGA, LSI, LPD, code pénal, LTrans, OPrI), les directives informatiques (par ex. directives concernant la sécurité informatique dans l'administration fédérale), les normes légales étrangères (par ex. RGPD, US CLOUD Act ou FISA américains) et l'obligation de garder le secret (par ex. secret de fonction, secret des affaires et secret professionnel).»

Le document s'adresse à toutes les unités de l'administration fédérale et - outre les juristes qui s'occupent des questions juridiques liées à l'utilisation du nuage - en particulier aux dirigeants et aux responsables de projets[8], auxquels incombe également le respect des aspects juridiques des projets nuagiques.

1.2 But du rapport

Le présent rapport présente de manière descriptive les domaines juridiques qui peuvent être importants pour les projets nuagiques et traite de manière synthétique les principales questions juridiques. Il met l'accent sur la protection et la sécurité des données, la protection des informations et le secret de fonction. Il doit d'une part clarifier des questions juridiques fondamentales pour l'approvisionnement infonuagique et créer ainsi une compréhension juridique uniforme pour l'administration fédérale. D'autre part, il doit montrer quels sont les moyens juridiques à disposition pour garantir la « conformité » des projets d'approvisionnement infonuagique. L'annexe C du présent rapport contient une liste des risques éventuels de l'approvisionnement infonuagique et les mesures envisageables pour les réduire à un niveau acceptable. Celles-ci doivent montrer de manière structurée aux unités administratives ce dont elles doivent tenir compte d'un point de vue juridique lors de projets nuagiques et ce qu'elles doivent vérifier au préalable afin d'être en conformité avec la loi.

Le présent rapport se limite aux domaines juridiques qui concernent l'ensemble de l'administration fédérale et n'aborde pas le droit spécial qui peut s'appliquer à un domaine spécifique. Il s'agit d'un document évolutif qui sera régulièrement mis à jour et complété.

Ses considérations sont en principe applicables à l'analyse des bases juridiques de tous les projets d'approvisionnement nuagiques, quel que soit le modèle ou le service.

2 Notions: modèles et services nuagiques

Le présent chapitre expose brièvement les modèles et les services du nuage afin de faciliter la compréhension du rapport. La stratégie d'informatique en nuage de l'administration fédérale prévoit cinq options d'approvisionnement : les centres de calcul de la Confédération, les nuages publics, un Swiss

[5] Le Conseil fédéral a alors décidé que les travaux relatifs au nuage du programme SUPERB seraient poursuivis indépendamment du calendrier de mise en œuvre de la stratégie. Ils sont adaptés au programme SUPERB au fur et à mesure. Les incohérences éventuelles sont corrigées dans la stratégie et dans le programme SUPERB.
[6] Stratégie d'informatique en nuage de l'administration fédérale (admin)
[7] D'autres mandats partiels, notamment l'élaboration d'e moyens auxiliaires, seront ensuite exécutés sur la base du présent rapport, probablement d'ici fin 2022.
[8] Notamment les préposés à la sécurité de l'information de la Confédération (DSID et DSIO).

Cloud, des nuages communautaires ou une externalisation classique[9]. La stratégie de la Confédération pour le réseau de centres de calcul prévoit elle aussi que les nuages publics doivent servent davantage de centres de calcul[10].

Il existe aujourd'hui quatre modèles principaux de déploiement de l'informatique en nuage[11] et trois modèles de services[12].

Les modèles de déploiement sont les suivants :
- les nuages publics,
- les nuages privés,
- les nuages hybrides, et
- les nuages communautaires.

Les trois modèles de services sont les suivants:
- Infrastructure en tant que service (Infrastructure as a Service; IaaS),
- Logiciel en tant que service (Software as a Service; SaaS), et
- Plateforme en tant que service (Platform as a Service (PaaS).

Les services peuvent prendre la forme d'une infrastructure, d'une plateforme ou d'un logiciel, hébergés par des fournisseurs tiers et mis à disposition des utilisateurs par Internet. C'est la manière dont ils sont mis à disposition qui différencie les services.

2.1 Modèles de déploiement de l'informatique en nuage[13]

Nuages publics

L'infrastructure en nuage est mise à disposition par le fournisseur de services nuagiques pour une utilisation ouverte au grand public. Il peut s'agir d'une entreprise, d'une université ou d'une organisation étatique, ou d'une combinaison des deux. L'infrastructure se trouve dans les locaux du fournisseur. Les plus grands fournisseurs de nuages publics sont à l'heure actuelle Amazon Web Services, Microsoft et Google[14].

Nuages privés

L'infrastructure en nuage est mise à la disposition exclusive d'une seule organisation (par ex. l'administration fédérale) comportant plusieurs utilisateurs (par ex. offices). Elle peut être détenue, gérée et exploitée par l'organisation, par un tiers (fournisseur de services nuagiques) ou par une combinaison des deux, et elle peut être « sur site » ou « hors site ». Le nuage Atlantica de la Confédération est un nuage privé.

Nuages hybrides

L'infrastructure en nuage comprend deux ou plusieurs infrastructures en nuage différentes (privées, communautaires ou publiques), indépendantes, mais reliées par une technologie standardisée ou propriétaire permettant la portabilité des données et des applications (par ex. éclatement pour équilibrer la charge entre les nuages).

Nuages communautaires

L'infrastructure en nuage est mise à la disposition exclusive d'une communauté ou d'un groupe d'utilisateurs spécifique ayant des intérêts communs (par ex. exigences en matière de sécurité, critères de conformité). Elle peut être détenue, gérée et exploitée par plusieurs organisations qui forment une communauté, par un tiers ou une combinaison des deux, et elle peut être « sur site » ou « hors site ».

[9] Cf. Stratégie d'informatique en nuage de l'administration fédérale
[10] Stratégie de la Confédération pour le réseau de centres de calcul (en cours d'élaboration).

[12] Voir plus haut.
[13] Les définitions sont tirées de: NIST SP 800-145, The NIST Definition of Cloud Computing.
[14] Magic Quadrant für Cloud-Infrastruktur und Plattform-Services (gartner.com)

2.2 Modèles de services en nuage[15]

Infrastructure en tant que service (IaaS),

Dans le modèle IaaS, un fournisseur met à disposition une infrastructure qui permet à l'utilisateur de disposer de ressources de traitement, de stockage, de réseau et d'autres ressources informatiques de base sur laquelle il peut déployer et exécuter n'importe quel logiciel, y compris des systèmes d'exploitation et des applications. L'utilisateur ne gère pas ou ne contrôle pas l'infrastructure sous-jacente, mais contrôle les systèmes d'exploitation, l'espace de stockage et les applications installées, et peut le cas échéant exercer un contrôle limité sur certains composants du réseau (par ex. les pare-feu hébergés).

Plateforme en tant que service (PaaS).

Dans le modèle PaaS, les produits fournis à l'utilisateur consistent à déployer dans l'infrastructure du nuage des applications créées ou achetées par l'utilisateur et créées à l'aide des langages de programmation, des bibliothèques, des services et des outils pris en charge par le fournisseur. L'utilisateur ne gère pas ou ne contrôle pas l'infrastructure sous-jacente, ni le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais contrôle les applications fournies et le cas échéant les paramètres de configuration de l'environnement d'hébergement des applications.

Logiciel en tant que service (SaaS)

L'utilisateur a la possibilité d'utiliser les applications du fournisseur qui fonctionnent sur une infrastructure nuagique. L'accès aux applications se fait à partir de différents appareils clients, soit par une interface client léger, telle qu'un navigateur web (par ex. messagerie web), ou par une interface de programmation. L'utilisateur ne gère pas ou ne contrôle pas l'infrastructure sous-jacente, ni le réseau, les serveurs, les systèmes d'exploitation ou le stockage ni même certaines fonctions des applications, à l'exception, le cas échéant, de paramètres de configuration des applications limités et spécifiques à l'utilisateur.

3 Aspects liés aux risques

Le choix d'un modèle ou d'un service nuagique présuppose - indépendamment des mesures contractuelles, organisationnelles et techniques appropriées à prendre en l'espèce - une confiance de base minimale dans la technologie infonuagique, dans le système juridique et dans le service concerné, que les fournisseurs de services respectent les contrats et qu'ils ne manipulent pas leurs systèmes au détriment des utilisateurs[16]. Chaque projet concret nécessite donc une analyse juridique et une évaluation des risques approfondies et critiques, sur la base desquelles les mesures d'atténuation nécessaires (contractuelles, techniques ou organisationnelles, cf. annexe C) seront définies.

Les modèles de nuages publics s'impliquent une externalisation des données. Les données ne sont pas stockées ni traitées dans des centres de calcul sur site (si les infrastructures du fournisseur de services sont utilisées).

Dans les modèles de nuages privés, il est possible que les données soient traitées dans des centres de calcul exploités par les fournisseurs de services, mais qu'elles soient utilisées exclusivement par un utilisateur particulier. Les centres de calcul de la Confédération entrent aussi dans cette catégorie, dans la mesure où l'unité administrative responsable du traitement des données n'est pas celle qui exploite les centres de calcul[17].

Outre le fait que l'unité administrative compétente n'a plus elle-même le contrôle physique des moyens informatiques, trois facteurs en particulier contribuent à la complexité juridique, mais aussi technique, des solutions d'approvisionnement infonuagique, ce dont il faut tenir compte lors de l'évaluation des risques :

- Lien avec l'étranger : les services des nuages publics peuvent être fournis à l'étranger comme en Suisse (emplacements des serveurs, accès au support). Plusieurs fournisseurs hypersca-

[15] Les définitions sont tirées de: NIST SP 800-145, The NIST Definition of Cloud Computing.
[16] Les fournisseurs de services le démontrent notamment par leurs certifications. Cf. David Rosenthal, Schweizer Banken in die Cloud.
[17] Le cadre juridique est cependant différent, notamment parce qu'une surveillance est en place au sein de l'administration fédérale, que la Confédération exerce un contrôle physique sur l'infrastructure et que les collaborateurs sont soumis à des dispositions légales plus strictes.

laires (par. ex.. AWS et Microsoft) disposent de centres de calcul en Suisse. Il est donc possible de définir techniquement, contractuellement et sur le plan conceptuel, que la conservation et le traitement des données doivent être effectués en Suisse (voir également l'annexe C)[18].

- Recours à des sous-traitants : pour l'exécution du mandat, les fournisseurs de services nuagiques (également pour les solutions de nuage privé) font généralement appel à d'autres tiers qui accomplissent certaines tâches[19]. Par ailleurs, ces sous-traitants exécutent parfois leurs tâches à partir de pays tiers. Dans ce cas, la conformité doit être garantie partout.

3.1 Évaluation des risques

L'utilisation de services de nuage public n'est pas la seule à comporter des risques. Certains risques existent également dans le modèle « sur site » traditionnel (l'exploitation a lieu dans les locaux de l'utilisateur, avec son matériel et avec son personnel), notamment le risque de cyberattaque ou de panne des infrastructures techniques (les infrastructures de réseau sont souvent exploitées ou entretenues en tout ou en partie par des tiers, par ex.), avec les risques de réputation qui y sont liés, ainsi que la possibilité que des données soient retirées des locaux de l'utilisateur[20].

Ces risques sont parfois accentués par les solutions nuagiques, mais aussi atténués dans certaines circonstances (la protection contre les cyberattaques peut être meilleure[21]). Les solutions nuagiques peuvent toutefois présenter de nouveaux risques. Toute solution (qu'elle soit « sur site » ou dans le nuage) exige que - dans le cadre juridiquement autorisé - ses risques inhérents soient maintenus, par des mesures adéquates, dans des limites proportionnées et donc acceptables par rapport aux avantages qu'elle procure (par ex. en termes d'efficacité et d'évolutivité). Cela vaut pour les solutions « sur site » comme pour les solutions de nuage public.

Schématiquement, les groupes de risques sont les suivants :

- Risques de conformité (risques juridiques au sens strict) : violation des prescriptions légales concernant la protection des données, la protection du secret, la protection de l'information, la sécurité des données et d'autres lois spéciales.
- Risques de continuité des activités et de reprise après sinistre : disponibilité de l'accès aux données propres, disponibilité des réseaux, intégrité des données, portabilité des données (effets de verrouillage[22]), sauvegarde hors du nuage. Il convient également de tenir compte, le cas échéant, des exigences du droit des marchés publics, qui peuvent avoir pour conséquence que les services nuagiques doivent faire l'objet d'un nouvel appel d'offres après un certain temps, conformément à la loi fédérale sur les marchés publics (LMP, RS 172.056.1)[23].
- Risques politiques (cf. aussi partie 2, ch. 1.7) : environnement juridique à l'étranger, par ex. restrictions à la libre circulation des données ; accès des autorités selon le droit étranger[24]; espionnage par des services de renseignement (en Suisse et à l'étranger) ; conflits à l'étranger.
- Risques de réputation : la confiance des citoyens dans l'administration fédérale peut être affectée en fonction du choix du fournisseur de services nuagiques, des données transférées dans le nuage ou des incidents potentiels.

Les risques typiques sont détaillés dans l'annexe C et comparés aux mesures d'atténuation qui s'y rapportent. Mais celles-ci ne peuvent généralement pas éliminer les risques existants, elles peuvent tout au plus les réduire adéquatement et assurer la résilience nécessaire si un risque se réalise.

3.2 Acceptation des risques

Il appartient à la direction de l'unité administrative responsable des données à transférer de décider quels sont les risques résiduels acceptables. Cette décision doit être prise en fonction de la nature des données à transférer sur la base d'une analyse des risques approfondie, dans le respect du droit applicable. L'analyse des risques doit tenir compte des facteurs de risque existants dans le cas concret et des mesures prises pour les atténuer.

[18] Voir aussi le ch. 2.6.
[19] Cf. NCSC, aide-mémoire «Public- oder Hybrid-Cloud-Nutzung in der Bundesverwaltung»,03/2021.
[20] https://www.swissinfo.ch/ger/anklage-macht-ausmass-des-diebstahls-beim-nachrichtendienst-bekannt/42586612, voir aussi FAQ concernant l'utilisation de technologies nuagiques 220826_VUD_FAQ zum Einsatz von Cloud.pdf).
[21] Il convient de vérifier au cas par cas si cela s'applique à un projet concret.
[22] Cf. NCSC, aide-mémoire, ch. 3; Millard, p. 43 s.
[23] Dans ce contexte, pour les solutions de nuage public OMC 20007, on retiendra que les contrats-cadres sont valables pour une durée de 5 ans.
[24] On parle parfois d'« accès légal ».

En fonction des résultats de l'analyse des risques concernant un projet concret, il faudra décider si le traitement des données peut être effectué dans un centre de calcul ou un nuage de la Confédération, dans un autre nuage privé exploité par des fournisseurs de services nuagiques, dans un nuage hybride ou dans un nuage public. L'annexe E présente schématiquement des modèles de déploiement infonuagique adéquats.

4 Accords contractuels avec des fournisseurs de services nuagiques

Les services responsables de l'administration fédérale doivent vérifier soigneusement que les conditions proposées dans les contrats-types des fournisseurs de services nuagiques correspondent au standard requis pour les données à traiter. Les fournisseurs hyperscalaires disposent souvent de constructions contractuelles complexes, qui doivent être examinées dans leur ensemble. Cela peut entraîner un surcroît de travail considérable et nécessiter l'acquisition de nouvelles compétences pour l'unité administrative concernée. Le cas échéant, il faudra imposer des adaptations, notamment en ce qui concerne les points suivants (voir également les mesures contractuelles mentionnées à l'annexe C) :

- Respect du secret de fonction (cf. partie 2, ch. 0),
- Traitement des données conforme aux instructions (cf. partie 2, ch. 1.3.2),
- Mesures de sécurité supplémentaires (cf. partie 2, ch. 1.2 et 1.3),
- Pouvoirs de contrôle, notamment en ce qui concerne les résultats des audits (voir partie 2, ch.1.3.2 et 1.5.1).

Même si des garanties contractuelles peuvent être obtenues, le risque de violation du contrat et les éventuels obstacles à leur détection par l'administration fédérale doivent toujours être pris en compte dans l'évaluation des risques.

5 Solutions nuagiques dans le cadre du modèle de gouvernance OMC 20007

L'Office fédéral des constructions et de la logistique (OFCL) et le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (TNI ChF) concluent avec les adjudicataires (fournisseurs de services nuagiques) de l'appel d'offres OMC (20007) 608 Public Clouds Bund[25], des contrats-cadres portant sur un volume total de prestations (plafond de coûts) de 110 millions de francs sur 5 ans. L'appel d'offres ne porte pas sur les contrats existants avec des fournisseurs de services nuagiques ni sur les prestations fondées sur des licences (c.-à-d. qui comprennent l'utilisation de logiciels, par ex. Microsoft M365/CEBA ou des solutions SAP en nuage).

Si une unité administrative souhaite utiliser une solution infonuagique, elle doit choisir le fournisseur le plus approprié dans le cadre d'un projet concret, en fonction d'un cahier des charges neutre et de critères d'examen prédéfinis (par ex. degré de réalisation des exigences techniques, conformité à la stratégie d'informatique en nuage, évaluation des risques [protection des données, sécurité de l'information, mesures organisationnelles et techniques associées], et d'une évaluation (les critères d'examen doivent être conformes aux exigences du cahier des charges de l'appel d'offres OMC). Les unités administratives choisiront la solution la mieux adaptée à leur projet, soit elles-mêmes, soit par l'intermédiaire d'un courtier de services en nuage (il est probable que ce sera principalement l'Office fédéral de l'informatique et de la télécommunication [OFIT] qui assumera cette fonction) avec le fournisseur de services nuagiques concerné. En principe, le choix se fait dans le cadre du contrat-cadre conclu avec le fournisseur concerné. Le volume commandé est imputé au volume total des services.

[25] Dossier d'appel d'offres disponible sur www.simap.ch; numéro de la publication 1202937

Partie 2 - Cadre juridique

L'utilisation de services nuagiques relève du domaine des activités administratives auxiliaires. Par activité administrative auxiliaire, on entend l'acquisition des biens matériels ou des prestations nécessaires à l'administration pour accomplir sa tâche publique[26]. L'achat de matériel de bureau, la conclusion de contrats d'entreprise pour la construction d'un bâtiment public ou le recours à un fournisseur de prestations informatiques en sont des exemples. En pareil cas, l'unité administrative conclut en principe des contrats de droit privé. La base légale découle directement de celle de la tâche publique concernée[27]. Toutefois, en fonction du domaine ou de la nature des données traitées, la base légale doit respecter des exigences particulières. C'est notamment le cas lorsque des données personnelles sont traitées dans le nuage.

1 Législation fédérale sur la protection des données

Lors du traitement de données à caractère personnel avec des solutions infonuagiques, les données seront le plus souvent sous-traitées au sens de la législation sur la protection des données. Par conséquent, dans la mesure où des données personnelles doivent être transférées dans le nuage ou traitées dans le cadre de services nuagiques (en particulier le modèle SaaS, cf. partie 1, ch. 2.1), les prescriptions de la législation sur la protection des données doivent être respectées.

La loi sur la protection des données a fait l'objet d'une révision totale en 2020. La nouvelle loi sur la protection des données (nLPD) et ses ordonnances d'application entreront en vigueur le 1er septembre 2023[28]. Le présent rapport se fonde en grande partie sur le futur droit, dont les exigences vont au-delà de celles du droit en vigueur.

La LPD définit les principes de la protection des données de manière générale et neutre sur le plan technologique. Le traitement concret et ses conditions-cadres sont précisés dans le droit spécial. Outre la LPD et ses ordonnances d'application, il faut donc toujours tenir compte des dispositions relatives à la protection des données du droit spécial.

C'est notamment le cas des art. 58 ss de la loi sur les épidémies (RS *818.101*), 13 de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (RS *360*), 60*c* de la loi sur les finances (RS *611.0*) ou 55 ss de la loi sur l'énergie (RS *730.0*).

La nLPD fixe les principes généraux du traitement des données personnelles aux art. 6 ss:

- tout traitement de données personnelles doit être licite (le traitement doit en particulier reposer sur des bases légales d'un niveau normatif et d'une densité normative suffisants).
- il doit être conforme au principe de la bonne foi;
- il doit être conforme au principe de la proportionnalité;
- les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée;
- elles doivent être traitées ultérieurement de manière compatible avec ces finalités;
- le traitement des données doit être conçu, sur le plan technique et organisationnel, de manière à respecter les prescriptions en matière de protection des données, en particulier les principes fixés à l'art. 6 (art. 7 nLPD).

1.1 Données personnelles et traitement des données

1.1.1 Définition des données personnelles

[26] HÄFELIN/MÜLLER/UHLMANN, Allgemeines Verwaltungsrecht, 8. A., ch. 1384; TSCHAN-NEN/ZIMMERLI/MÜLLER, Allgemeines Verwaltungsrecht, 4. A., par. 4 N 8 ss

[27] Selon JAAG, qui se réfère aux auteurs susmentionnés, la doctrine et la pratique s'accordent sur le fait qu'une base légale spécifique n'est pas nécessaire dans le domaine des activités administratives auxiliaires. Il suffit que la tâche à laquelle servent les activités auxiliaires se fonde sur une base légale suffisante. La justification d'une tâche confère également la compétence de se procurer les moyens nécessaires à sa réalisation. Cela vaut également pour la compétence de confier à des tiers la mise à disposition des moyens nécessaires (externalisation) (cf. Bedarfsverwaltung, in: Sethe et al., Kommunikation. Festschrift für Rolf Weber zum 60. Geburtstag, 543 à 557, en particulier 554).

[28] : RO 2022 491; autres documents (en particulier le projet d'ordonnance mis en consultation): https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html

Sont des données personnelles au sens de la LPD toutes les informations concernant une personne identifiée ou identifiable sans que cela nécessite des efforts disproportionnés (art. 5, let. a, LPD). Les données qui répondent à cette définition ne peuvent être traitées que dans le respect des dispositions de la législation sur la protection des données. Les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale.

La LPD définit également des catégories de données dont le traitement est soumis à des exigences plus strictes concernant la base légale, à savoir les données sensibles (art. 5, let. c, nLPD). En règle générale, le traitement des données sensibles doit se fonder une loi fédérale. Sont des données sensibles:

- les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
- les données sur la santé, la sphère intime,
- l'origine raciale ou ethnique,
- les données génétiques,
- les données biométriques identifiant une personne physique de manière univoque,
- les données sur des poursuites ou sanctions pénales et administratives,
- les données sur des mesures d'aide sociale.

La loi prévoit des règles plus strictes pour le *profilage* (cf. art. 34 nLPD). Par profilage, on entend toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique (art. 5, let. f, nLPD).

Par profilage à risque élevé, on entend tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (art. 5, let. f, nLPD).

1.1.2 «Traitement de données personnelles»

1.1.2.1 Définition du « traitement »

Par *traitement*, on entend toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, *notamment* 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)[29].

1.1.2.2 Conditions préalables au traitement des données personnelles

En règle générale, une ordonnance suffit comme base légale pour le traitement de données personnelles, à moins qu'il ne s'agisse de données sensibles. Le traitement de celles-ci nécessite en règle générale une base légale dans une loi fédérale (cf. partie 1, ch. 1.1.1).

Pour les unités administratives, le *profilage* n'est en principe autorisé que sur la base d'une base légale au sens formel (art. 34, al. 2, let. b, nLPD) (cf. ch. 1.1.1). Par loi au sens formel on entend un acte qui a rang de loi dans le droit fédéral (une ordonnance ne suffit pas). Les exigences en matière de densité normative sont aussi relativement élevées. La loi doit être formulée de manière suffisamment claire et précise, notamment en ce qui concerne les données utilisées, le but et les conditions, ainsi que les modalités du profilage, pour que l'atteinte aux droits fondamentaux des personnes concernées soit prévisible pour celles-ci.

1.1.3 «Données concernant des personnes morales»

Dans le droit en vigueur, les données concernant des personnes morales sont considérées comme des données personnelles. Les données des personnes morales n'entrent plus dans le champ d'application de la nLPD.

[29] En ce qui concerne le traitement par les fournisseurs de services nuagiques, voir le ch. 2.5.

La révision du 25 septembre 2020 de la LPD prévoit l'inscription des bases légales du traitement des données concernant des morales aux art. 57*r* ss de la loi du 21 sur l'organisation du gouvernement et de l'administration (LOGA ; RS *172.010*). Ces dispositions s'appuient ponctuellement sur la nLPD[30].

Les données de personnes morales peuvent être *traitées* par une unité administrative dans la mesure où l'accomplissement de sa tâche l'exige et dans la mesure où ses tâches dont définies dans une loi au sens formel (art. 57*r*, al. 1, nLOGA). Cela vaut également pour les données sensibles de personnes morales. Si ces exigences sont remplies, il n'est pas nécessaire de prévoir une habilitation dans une loi spéciale, sauf si le traitement des données aboutit à une atteinte très grave aux droits fondamentaux de la personne morale concernée.

Conformément à l'art. 57*r*, al. 2, nRVOG, les données sensibles concernant des personnes morales sont :

- les données relatives à des poursuites ou des sanctions administratives ou pénales,
- les données relatives à des secrets professionnels, d'affaires ou de fabrication.

La *communication* de données concernant des personnes morales est soumise à des règles plus strictes. L'art. 57*s*, al. 1, nLOGA prévoit que la communication de données concernant des personnes morales requiert une base légale dans une loi spéciale. Pour les données ordinaires, une disposition d'ordonnance suffit en règle générale ; par contre, pour les données sensibles, une base dans une loi au sens formel est en principe nécessaire[31].
Cette condition devrait donc être respectée pour les solutions nuagiques, par exemple lorsque des données relatives à des secrets professionnels, d'affaires ou de fabrication sont traitées. La communication de telles données nécessite en outre que d'autres mesures de protection soient prises. Elles devraient être pseudonymisées ou au moins cryptées adéquatement pour les phases « données en transit » et « données au repos » (cf. partie 2, ch. 1.2.2). Il convient également d'examiner les mesures de protection adéquates (par. ex. accès limité ou traitement protégé des données[32]) pour la phase « données en cours d'utilisation »[33].

1.2 Approches techniques de la protection des données

Il existe différentes approches pour protéger les données contre un accès ou une consultation non autorisés. Dans le contexte du nuage, la dépersonnalisation (anonymisation et pseudonymisation), la tokenisation et (avec certaines restrictions) le cryptage des données sont cruciaux.

1.2.1 Anonymisation et pseudonymisation des données

L'anonymisation consiste à supprimer définitivement toutes les données identifiantes. Elle doit être irréversible. L'anonymisation n'est donc envisageable que lorsque l'identité de la personne ne joue plus aucun rôle, par exemple à des fins statistiques. Leur traitement n'est alors plus soumis à la loi sur la protection des données. L'anonymisation complète peut être techniquement difficile à réaliser, car des tiers peuvent, dans certaines circonstances, rétablir un lien avec une personne au moyen de méthodes analytiques, lorsque les données sont apparemment anonymes[34]. En conséquence, une anonymisation complète peut nécessiter des interventions si radicales dans les données que celles-ci ne peuvent plus adaptées à leur finalité.

La *pseudonymisation* consiste à remplacer l'ensemble des données identifiantes par un identifiant neutre (pseudonyme). En règle générale, certains éléments des jeux de données sont remplacés par des caractères, par exemple les noms par des numéros (procédé analogue à la « tokenisation »[35]). L'organe responsable dispose d'une table de correspondance. Mais, en règle générale, la pseudonymisation rend simplement plus difficile le rétablissement d'un lien avec une personne. Si des

[30] Cf. OFJ, Révision totale de la loi fédérale sur la protection des données (LPD). Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux, ch.. 3.2 (projet).
[31] Dans certaines conditions, une ordonnance peut également suffire, notamment lorsque la communication de données est indispensable à l'accomplissement d'une tâche réglée par une loi au sens formel et que le but du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne morale concernée (OFJ, Révision totale de la LPD, ch. 3.2.3). Toutefois, il est peu probable qu'une solution nuagique et la communication qui lui est liée soient « indispensables ». Les exceptions et cas spéciaux prévus à l'art. 57*s* concernent des communications dans des cas d'espèce et ne s'appliquent pas aux solutions nuagiques.
[32] Par exemple, la technologie « Confidential Computing » (informatique confidentielle), dans lequel les données sensibles sont isolées pendant le traitement dans des processeurs protégés ; voir par exemple https://www.ibm.com/cloud/learn/confidential-computing.
[33] On a manifestement oublié de transférer l'art. 9 nLPD dans la LOGA pour les données des personnes morales. A notre avis, le privilège de la communication à des sous-traitants selon l'art. 9 nLPD s'applique néanmoins (lacune). Un durcissement par rapport à la réglementation actuelle n'était manifestement pas voulu. En soi, l'utilisation d'une solution nuagique ne nécessite donc pas une base légale.
[34] Cf. à ce sujet WIDMER, p. 9.
[35] Cf. MILLARD, p. 38.

tiers disposent de données ou d'informations contextuelles, il leur est possible, dans certaines circonstances, d'attribuer les données aux personnes concernées. Une pseudonymisation est suffisante lorsque, compte tenu des circonstances, le risque semble faible que des tiers ne disposant pas de la table de correspondance soient en mesure, moyennant un effort raisonnablement prévisible[36], de réattribuer les données à des personnes. Dans ce cas, les dispositions de la nLPD ne s'appliquent pas aux tiers.[37]

D'un point de vue juridique, l'anonymisation et la pseudonymisation ont pour conséquence qu'il n'est pas possible d'accéder au texte en clair et qu'il n'y a donc pas de communication de données à des tiers (parce qu'il ne s'agit justement plus de données personnelles, étant donné que le fournisseur de services nuagiques ne peut plus remonter à une personne concrète).

La tokenisation est un procédé par lequel une partie identifiante des données est convertie en une chaîne de caractères aléatoires, appelée jeton (token). Un jeton n'a pas de valeur et ne sert que de substitut aux données proprement dites. Ce jeton est stocké, par exemple, dans une base de données nuagique. Les jetons ne peuvent en aucun cas être utilisés pour accéder aux données d'origine. En effet, contrairement au cryptage, la tokenisation n'utilise pas de méthode cryptographique pour convertir les données en une forme cryptée (chiffrement). La tokenisation est notamment utilisée dans les systèmes de paiement sécurisés.

1.2.2 Cryptage

Lors du *cryptage*[38], les données sont modifiées de manière à ce que la référence personnelle - ou le contenu informatif des données en général - ne soit pas visible pour des tiers qui ne disposent pas d'une clef. Tant que le cryptage est fiable ou suffisamment fort et que les clefs sont secrètes, seul le détenteur des clefs peut récupérer les données.

L'utilité du cryptage pour garantir la protection et la sécurité des données varie en fonction de la phase de traitement et de la norme de cryptage. La gestion des clefs[39], qui offre une garantie élevée que les objectifs poursuivis par le cryptage peuvent être atteints, est cruciale à cet égard. Il convient de clarifier qui gère effectivement la clef, si la clef est partagée (si une personne ne connaît que la moitié de la clef ou dispose d'une deuxième clef). →Double Key Encryption), comment éviter la perte de la clef ou comment récupérer les clefs (Key Recovery). Sinon, des données pourraient être perdues. Il faut également tenir compte du fait que la technologie évolue rapidement et que le cryptage devra, le cas échéant, être adapté à l'état actuel de la technique. Il existe différentes approches de gestion des clefs. En principe, il faut adopter des solutions dans lesquelles les personnes qui sous-traitent les données (fournisseurs de services nuagiques, hébergeurs de nuages, autres prestataires de services ; cf. partie 2, ch. 1.2.2) n'ont pas accès aux clefs, ou seulement un accès très limité (par ex. « Bring Your own Key » en utilisant un module de sécurité dédié dans le nuage ou « Keep your own Key »)[40]. Il en va de même pour d'autres approches visant à protéger les données contre une consultation non autorisée, par exemple en limitant les droits d'accès et en utilisant des systèmes de sécurité ou d'authentification complémentaires (voir annexe C).

Les technologies de cryptage évoluent constamment, il faut donc veiller à ce la solution de cryptage choisie corresponde toujours à l'état actuel de la technique. Il faut également tenir compte de l'horizon temporel, car les techniques de cryptage sûres aujourd'hui peuvent ne plus l'être à l'avenir. Les méthodes de cryptage varient en fonction de l'état des données. Il convient notamment de vérifier si les normes de cryptage utilisées ainsi que les mesures de protection des clefs sont suffisantes[41]. Les solutions de cryptage, en particulier les architectures de gestion des clefs, peuvent être conçues de différentes manières et mises en œuvre à différents stades du traitement des données, selon que celles-ci sont transportées d'un ordinateur à un autre *(données en transit*), traitées *(données en cours d'utilisation*) ou stockées dans un environnement en nuage *(données au repos*).

Données en transit

[36] L'ampleur des efforts qu'un pirate pourrait raisonnablement fournir doit toujours être examinée au cas par cas dans le cadre de l'évaluation des risques et dépend de différents facteurs (notamment des autres données disponibles pour une réidentification). L'évaluation peut changer en fonction de l'évolution technique.
[37] Cf. à ce sujet WIDMER, p. 10.
[38] Concernant le cryptage, voir aussi NCSC, Nutzbarkeit von Cloud-basierten Dienstangeboten in der Bundesverwaltung, du 8 novembre 2021.
[39] Pour un aperçu, voir NCSC, op. cit. p. 3.
[40] Dans le cadre de l'appel d'offres OMC 20007, une garantie correspondante a été exigée; cf. catalogue des exigences, p. 8 (ST03) ; cf. également DAVID ROSENTHAL, Schweizer Banken in die Cloud ; concernant les différentes approches de la gestion des clefs, cf. NCSC, op. cit. p. 3.
[41] On peut même imaginer des scénarios dans lesquels un cryptage de bout en bout pourrait conduire à ce qu'aucune donnée ne soit communiquée, par exemple en cas de simple hébergement de données dans le nuage.

Il existe diverses technologies pour protéger la transmission des données. Les données peuvent être transmises sous forme cryptée ou au moyen d'une gestion sécurisée des données (par ex. via SFTP, HTTPS via TLS ou VPN). SCION, est une nouvelle technologie suisse qui garantit la sécurité de la transmission des données (routage) de manière automatisée[42]. En plus du cryptage, les CASB (Cloud Access Security Brokers, courtiers de sécurité d'accès au nuage) offrent une couche supplémentaire de protection. Il s'agit de systèmes de sécurité qui vérifient de manière automatisée le respect des consignes de sécurité et peuvent éventuellement bloquer des données pour certains utilisateurs si ceux-ci ne respectent pas les normes de sécurité prescrites. Les passerelles qui automatisent le cryptage, la pseudonymisation ou la tokenisation peuvent également être servir de mesures de protection[43].

Données au repos

Les données ne sont ni traitées ni accessibles. Elles sont stockées, par exemple sur un serveur. Les données au repos sont relativement faciles à protéger. Elles peuvent être cryptées, sur un disque dur, dans des fichiers ou dans des banques de données. Elles peuvent aussi être protégées par CASB. Cependant, dès qu'elles sortent du nuage, la protection par CASB ne peut plus être garantie. Si la clef est détenue par le fournisseur de services nuagiques ou l'hébergeur (selon le type de gestion des clefs), l'accès ne peut pas être totalement exclu.

Données en cours d'utilisation

Il s'agit de données stockées en mémoire et utilisées activement par un logiciel. Les données en cours d'utilisation sont les plus vulnérables, car elles doivent être décryptées pour être traitées et sont alors stockées dans la mémoire de travail. À ce stade aussi, il est possible de protéger les données contre un accès non autorisé. D'une part, par des outils de gestion des identités et, d'autre part, par la gestion des droits d'information (IRM). Les outils de gestion des identités permettent de restreindre et de contrôler le cercle des personnes autorisées à traiter les données. L'IRM limite les traitements des données que l'agent peut effectuer. Ces données ne peuvent par exemple pas être imprimées ou modifiées. L'utilisation de matériel de confiance est une autre mesure de protection possible (*Trusted Execution Environment* [TEE] ou *Secure Enclave*)[44]. L'informatique confidentielle est une nouvelle technique qui empêche les fournisseurs de services nuagiques d'accéder aux données pendant leur traitement[45].

Dans l'état actuel de la technique, le risque d'accès aux données par des personnes non autorisées est en général le plus probable dans la phase *données en cours d'utilisation*[46]. Une combinaison des différentes mesures de protection permet toutefois de réduire le risque. L'analyse des risques doit montrer dans le cas d'espèce quelles sont les mesures de protection des données les plus appropriées et si les mesures possibles sont globalement suffisantes pour garantir une protection adéquate et conforme à la loi (voir annexes C à E).

1.3 Sécurité des données

1.3.1 Principes

L'art. 8 nLPD impose aux responsables du traitement et aux sous-traitants l'obligation de garantir une sécurité une sécurité adéquate des données par rapport au risque encouru, par des mesures organisationnelles et techniques appropriées. Les mesures doivent permettre d'éviter toute violation de la sécurité des données.

Le projet d'ordonnance relative à la loi fédérale sur la protection des données pose des principes concernant[47]:

- les objectifs de protection (confidentialité, disponibilité, intégrité),

[42] Seule l'application passerelle à passerelle *Broad Network Access* n'est pas supportée pour le moment, notamment parce que les terminaux ne sont pas supportés par un agent SCION. Informations complémentaires sur SCION : SCION Internet Architecture (scion-architecture.net).
[43] De nouvelles approches telles que *Secure Access Service Edge* (SASE) peuvent également être utilisées, y compris *Zero Trust Network Access* (ZTNA). Voir également MILLARD, p. 38.
[44] Cf. NCSC, op. cit., p. 3 ; MILLARD, Cloud Computing Law, p. 39 s.
[45] Cf. NCSC Considérations technologiques.
[46] Dans la mesure où les données au repos et en transit sont cryptées et que le fournisseur de services infonuagiques n'a pas automatiquement accès aux clefs.
[47] Cf. également le guide correspondant du PFPDT : https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2018/TOM.pdf.download.pdf/guide TOM_fr_2015.pdf; ainsi que GA WIDMER, p. 15.

- les risques à prendre en compte (notamment la destruction accidentelle ou non autorisée, la perte accidentelle, les erreurs techniques, la falsification, le vol et l'utilisation illicite, ainsi que la modification, la copie, l'accès et les autres traitements non autorisés),
- les critères selon lesquels les mesures à prendre doivent être évaluées (finalité du traitement des données, nature et étendue des données concernées et du traitement des données prévu, risques éventuels pour les personnes concernées, état actuel de la technique).

Des prescriptions relatives à la sécurité des données figurent également dans d'autres actes (cf. partie 2, 0 et 4.2, notamment l'ordonnance sur les cyberrisques (OPCy)[48], la loi sur la sécurité de l'information (LSI)[49] et l'ordonnance concernant la protection des informations (OPrI), qui a effet jusqu'à l'entrée en vigueur de la LSI. Des directives règlent également des aspects de sécurité, par exemple concernant l'utilisation d'appareils mobiles ou la protection informatique de base[50].

Si, malgré toutes les mesures prises, la sécurité des données devait être violée, l'art. 24 nLPD prévoit en outre une obligation d'annonce qui concerne expressément aussi les sous-traitants.

1.3.2 Règlement de traitement

Les mesures doivent être réglées en détail dans un règlement de traitement[51] (art. 5, al. 2, en relation avec l'art. 6, al. 2, OPDo). Ce règlement doit être établi lorsque les conditions de l'art. 6, al. 1, OPDo sont réunies. Les mesures techniques disponibles pour l'utilisation du nuage public sont généralement définies par le fournisseur de services nuagiques concerné. Les procédés utilisés peuvent parfois être choisis dans un catalogue de services (dont dépendent les licences et les coûts). Ils doivent aussi être documentés (voir aussi l'annexe C). Le règlement de traitement doit définir en premier lieu les mesures organisationnelles, c'est-à-dire qui peut traiter quelles données et comment (et le cas échéant quand et à quelle fréquence). Les mesures techniques offrant une protection suffisante doivent également être évaluées en fonction de l'état actuel de la technique et peuvent donc évoluer.

Pour les solutions nuagiques, il convient de mentionner les principaux risques suivants en matière de sécurité des données, qui doivent faire l'objet de mesures techniques et organisationnelles appropriées et pour lesquels - dans la mesure du possible - des réglementations contractuelles adéquates[52] doivent être prévues (y compris des règles sur la responsabilité ou les peines conventionnelles ; voir également l'annexe C pour l'ensemble)[53]:

- Manque de clarté de la réglementation des exigences de conformité et du traitement des incidents de sécurité (en particulier l'annonce des incidents liés à la sécurité) : les exigences de conformité (en particulier le respect des certifications, la divulgation des résultats des audits) doivent être fixées par contrat ; les contrôles correspondants doivent être effectués. Il en va de même pour l'obligation d'annoncer les incidents ayant une incidence sur la sécurité et la protection des données (voir également l'art. 24 nLPD)[54].
- Manque de clarté des réglementations organisationnelles dans le domaine de la responsabilité partagée : des TCR claires doivent être convenues, également dans le domaine de la sécurité du nuage (par ex. interactions avec le fournisseur de services nuagiques).
- Traitement de données sur des infrastructures utilisées en commun avec des bénéficiaires de prestations « étrangers », ce qui augmente notamment le risque de défaillance de l'isolation des données en cas de simple séparation logique plutôt que physique : convenir d'infrastructures physiquement séparées ; modèles d'architecture particuliers.
- Clarifier les possibilités de cryptage des données. Quels sont les différents types de cryptage ? Les données en transit et les données au repos peuvent-elles être cryptées de manière adéquate ? Où sont les clefs ? Qui a accès aux clefs ?
- Manque de disponibilité, par exemple en raison d'un manque de capacité du réseau, de lacunes dans la collaboration entre le fournisseur de services nuagiques, l'hébergeur et l'utilisateur ou d'un manque de protection chez le fournisseur contre les phénomènes naturels, les pénuries d'électricité ou autres : réglementation contractuelle et, le cas échéant, contrôles sur place.

[48] L'ordonnance sur les cyberrisques sera abrogée et certains de ses éléments intégrés dans la LSI et l'OSI.
[49] Entrée en vigueur : 1er mai 2022
[50] NCSC, Si001 – Protection informatique de base dans l'administration fédérale du 1er mars 2022 (https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/vorgaben/sicherheit/si001/Si001-IT-Grundschutz-V5-0-f.pdf); E026 Directive d'application sur le système de poste de travail, en particulier. 2.3 à 2.5.
[51] Cf. https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2014/06/was_muss_in_einembearbeitungsreglementaufgefuehrtwerden.pdf
[52] Pour les services nuagiques acquis au moyen de l'appel d'offres OMC 20007, les contrats-cadres conclus avec les prestataires mentionnent les mesures techniques disponibles. Le cas échéant, d'autres mesures peuvent être convenues.
[53] Voir également l'annexe C.
[54] Cet aspect a été défini au ch. 8.1 de l'appel d'offres OMC 20007.

- Espionnage informatique au moyen de matériel compromis: il est difficile d'évaluer dans quelle mesure ce risque est plus grand (ou même plus petit) par rapport aux solutions « sur site », car il existe aussi dans une certaine mesure lors du traitement avec son propre matériel.

Sur cette base, d'autres risques liés à la sécurité peuvent être identifiés et doivent être vérifiés:

- Dépendance vis-à-vis du fournisseur, migration des données plus difficile ou portabilité des données limitée, notamment en cas de fin de la collaboration : exiger des garanties contractuelles (interfaces, garantie des ressources au moyen de peines conventionnelles).
- Manque de personnel disposant d'une expertise adéquate (en particulier chez le mandant): exiger des garanties contractuelles.
- Risques de sécurité dus à des collaborateurs malveillants chez le fournisseur de services nuagiques ou dus à des sous-traitants mandatés par ce dernier (attaques internes) : restrictions d'accès, selon les données concernées : accord contractuel sur des contrôles de sécurité conformes aux normes en vigueur dans l'administration fédérale.

1.4 Avant l'utilisation d'un service en nuage: éventuelle analyse d'impact relative à la protection des données

L'art. 22, al. 1, nLPD prévoit que le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Cet instrument doit permettre d'identifier les risques à un stade précoce et de prendre d'éventuelles mesures de protection. Au sens de l'art. 22, al. 1, nLPD un risque élevé existe notamment dans le cas d'un traitement de données sensibles à grande échelle. L'analyse d'impact doit contenir une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures de protection prises ou prévues (art. 22, al. 3, nLPD). Le PFPDT doit être consulté si, malgré les mesures prévues, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 23, al. 1, nLPD).

En ce qui concerne les projets d'informatique en nuage, cela signifie que les risques liés à la protection des données doivent être déterminés au moyen de l'analyse d'impact relative à la protection des données (voir également l'annexe D) avant que des données permettant potentiellement d'identifier des personnes puissent être transférées dans le nuage, si le traitement de données prévu est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. La manière dont l'analyse d'impact relative à la protection des données doit être réalisée et la possibilité de l'intégrer dans des instruments existants (par ex. l'analyse des besoins de protection) sont en cours d'examen et seront définies par la pratique.

1.5 L'utilisation d'un service nuagique implique-t-elle un traitement des données par un sous-traitant ?

1.5.1 Sous-traitance du traitement des données dans la nLPD

L'art. 9 nLPD règle la sous-traitance du traitement de données personnelles. Le traitement de données personnelles peut être confié à un sous-traitant pour autant qu'un contrat ou la loi le prévoie, si seuls sont effectués les traitements que le responsable du traitement serait en droit d'effectuer lui-même[55]. Le sous-traitant ne peut pas traiter les données à des fins personnelles[56].

L'unité administrative reste responsable, car c'est elle qui décide - conformément à la base légale du traitement - comment ou avec quels moyens les données sont traitées (art. 9, al. 2, nLPD). Elle doit choisir, instruire et contrôler (dans la mesure du possible ou prévue par le contrat) avec soin les sous-

[55] Cf. 10*a* LPD, par ex. BAERISWYL in: le même / Pärli, Datenschutzgesetz (DSG), Berne 2015, art. 10a, N 14 ss).
[56] Les contrats-types des fournisseurs de services nuagiques peuvent prévoir que de tels traitements peuvent être effectués à des fins personnelles. Dans ce cas, ce traitement devrait être exclu par contrat, cf. ROSENTHAL, Schweizer Banken in die Cloud; souvent, de tels traitements sont effectués à des fins propres au sous-traitant, uniquement sur la base de données préalablement anonymisées ou pseudonymisées, et ils servent en fin de compte à nouveau les objectifs du mandant puisqu'ils améliorent la sécurité ou la qualité du service. Il convient alors de décrire précisément dans quelle mesure, par exemple, une analyse des données personnelles transmises est nécessaire et licite pour la fourniture des services nuagiques.

traitants et donc s'assurer activement qu'ils respectent les exigences de la protection des données comme elle devrait le faire elle-même.

Un service fédéral, en qualité de responsable du traitement, doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données personnelles. Il a donc une obligation de garantie. Cette garantie ne peut être mise en œuvre que si des contrôles réguliers sont effectués, par exemple par le biais d'un audit.

La loi prévoit en outre expressément que le sous-traitant ne peut confier le traitement à un tiers qu'avec l'autorisation écrite préalable du service fédéral responsable (art. 9, al. 3, nLPD). Celle-ci peut également être accordée au préalable, par exemple dans le contrat conclu avec le fournisseur de services nuagiques. Dans ce cas, un droit d'opposition doit être accordé au service fédéral afin qu'il puisse refuser de telles sous-sous-traitances. Les fournisseurs de services nuagiques recourent souvent à des sous-sous-traitants (par ex. pour l'hébergement physique des données, pour des services de réseau ou pour l'entretien et la maintenance ; cf. ch. 1.5.3).

En plus de la loi sur la protection des données, l'art. 11 de l'ordonnance sur la transformation numérique et l'informatique (OTNI; RS *172.010.58*) règle l'accès aux données pour les fournisseurs externes de prestations[57]. Ces derniers peuvent obtenir l'accès à des données qui ne sont pas accessibles au public si les conditions suivantes sont réunies :

- cet accès est *nécessaire* pour fournir la prestation (en d'autres termes, les données doivent impérativement être disponibles pour le prestataire afin qu'il puisse exécuter son mandat, ou cela représenterait un effort disproportionné s'il devait le faire sans avoir accès aux données ou uniquement sous une forme dépersonnalisée ou cryptée) ;
- l'autorité responsable des données a donné son accord par écrit (si elle rend elle-même les données accessibles et non son fournisseur de prestations interne, par exemple, l'accord visé à l'al. 1, let. b, relève de la compétence de l'autorité supérieure) ;
- des mesures contractuelles, organisationnelles et techniques appropriées ont été prises pour éviter que les données soient accessibles à des tiers.

1.5.2 Sous-traitance du traitement des données dans le contexte du nuage

Le fournisseur de services nuagiques n'est pas forcément un sous-traitant. Son statut dépend notamment du modèle choisi (par ex. SaaS, cf. partie 1, ch. 2.1).

Il convient de clarifier dans le cas d'espèce dans quelle mesure les données transférées dans le nuage sont effectivement sous-traitées par le fournisseur de services. En règle générale, il ne pourra accéder aux données en clair et les traiter lui-même que dans des cas très précis et convenus à l'avance. L'accès aux données secondaires, en particulier, fait exception à cette règle, car elles sont généralement collectées et traitées par fournisseur de services nuagiques pour la facturation de ses services.

1.5.3 Recours à des sous-traitants par le fournisseur de services nuagiques

Pour accomplir ses tâches, le fournisseur de services nuagiques fera souvent appel à des sous-traitants. Ceux-ci assurent souvent des fonctions clefs, que ce soit dans l'hébergement physique des données (hébergement nuagique du fournisseur de services), dans la transmission des données (exploitants de réseaux) ou dans le domaine de la maintenance ou du dépannage (support). Il peut s'avérer nécessaire que les sous-traitants aient accès à des données non cryptées pour pouvoir fournir une assistance. Il faut donc s'assurer que les tiers qui sont soumis au fournisseur de services nuagiques en tant que sous-traitants soient liés par les mêmes règles que le fournisseur de services lui-même (cf. art. 9 nLPD et 11 OTNI). Le contrat doit impérativement le prévoir. Le cas échéant, des mesures supplémentaires sont nécessaires.

[57] Il ne s'agit pas ici de la protection des données à proprement parler, mais de la protection du secret, cf. ch. 2.2.

1.6 Communication de données à l'étranger

1.6.1 Principes

Les art. 16 ss nLPD règlent la communication de données personnelles à l'étranger. Des données personnelles peuvent être communiquées à l'étranger si le Conseil fédé-ral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat (art. 16, al.. 1, nDSG)[58]. Ces États figurent dans l'annexe 1 OPDo. Actuellement, les États membres de l'UE, le Royaume-Uni, l'Argentine et la Nouvelle-Zélande remplissent ces conditions, contrairement aux États-Unis et à la Chine.

En outre, dans certains cas exceptionnels, des données peuvent être transmises à des États qui ne disposent pas d'un niveau de protection des données adéquat, notamment lorsque la personne concernée a expressément consenti à leur communication (art. 17, al. 1, let. a, nLPD). Il convient toutefois de souligner que les solutions de consentement pour les traitements systématiques de données ne constituent pas une solution appropriée en raison des exigences élevées en la matière (cf. art. 6, al. 6 et 7, nLPD).

Si, exceptionnellement, un traitement de données est nécessaire dans un État qui ne dispose pas d'une législation adéquate en matière de protection des données, il convient de prévoir une garantie contractuelle appropriée, par exemple au moyen de clauses contractuelles standard approuvées ou mises à disposition par le PFPDT[59] ou des garanties spécifiques élaborées par l'unité administrative compétente et communiquées au préalable au PFPDT[60]. En outre, des mesures techniques et organisationnelles appropriées doivent également être prises, par exemple un cryptage des données qui exclut dans une large mesure l'accès au contenu personnel des données par le sous-traitant (étranger) et les éventuels sous-sous-traitants[61]. Le cas échéant, il convient d'examiner s'il est possible d'établir des directives pour les « données en transit », par exemple en ce qui concerne le routage[62] (cf. partie 2, ch. 1.2.2).

Il faut également tenir compte, lors de la collecte de données personnelles, du devoir d'information particulier prévu à l'art. 19, al. 4, nLPD, lorsque des données sont communiquées à l'étranger et qu'il n'existe pas de législation adéquate en matière de protection des données dans l'État destinataire. Dans la mesure où le traitement n'est pas prévu par la loi (art. 20, al. 1, let. b, nLPD ; ce qui est toutefois une condition générale pour les autorités), les personnes concernées doivent être informées de l'État destinataire et, le cas échéant, des garanties prévues à l'art. 16, al. 2, nLPD. L'art. 20, al. 2, nLPD prévoit une exception à cette règle, lorsque l'information est impossible à donner ou qu'elle nécessite des efforts disproportionnés.

1.6.2 Dans le contexte du nuage

Il convient d'examiner dans le cas d'espèce s'il y a communication de données au sens de la LPD dans le cas de l'approvisionnement infonuagique[63]. Ce n'est pas le cas, par exemple, lorsque les données sont pseudonymisées ou tokenisées (cf. ch. 1.2.2) ou lorsque d'autres mesures sont prises pour exclure la consultation du contenu des données ou du « texte en clair » par le fournisseur de services nuagiques.

Les fournisseurs de services nuagiques doivent être tenus par contrat de se conformer de manière générale au droit suisse et en particulier aux dispositions relatives à la protection des données ; le for doit en principe être la Suisse[64].

Lors de l'utilisation de solutions nuagiques, le fournisseur de services doit s'engager auprès de l'utilisateur à ce que les données ne soient traitées et stockées que dans l'État étranger ou dans les États étrangers désignés par l'utilisateur du nuage[65]. Le fournisseur de services nuagiques doit indiquer

[58] La publication de données personnelles au moyen de services d'information et de communication automatisés afin d'informer le public (par ex. sites Internet de l'administration fédérale) n'est pas assimilée à une communication à l'étranger, même si ces données peuvent être consultées depuis l'étranger (art. 18 nLPD).
[59] Contrat-type pour l'externalisation (outsourcing) du traitement de données à l'étranger (admin.ch). Une exigence correspondante a été prévue dans l'appel d'offres OMC 20007 ; cf. catalogue des exigences, p. 12 (CAd03)
[60] Voir à ce sujet le guide de juin 2021 du PFPDT pour vérifier l'admissibilité des transferts directs ou indirects de données vers l'étranger (Transmission à l'étranger (ad https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-629182963min.ch)).
[61] On peut se demander s'il s'agit vraiment d'une « communication » lorsque le fournisseur de services nuagiques ne doit ou ne peut pas traiter lui-même les données et que son accès à celles-ci peut être largement exclu.
[62] Par exemple, l'utilisation de la norme SCION pourrait être obligatoire.
[63] Voir également à ce sujet, par exemple, BAERISWYL in: le même / Pärli, Datenschutzgesetz (DSG), Berne 2015, art. 10*a*, n. 43.
[64] Cf. pour l'appel d'offres OMC 20007: cf. cahier des charges, ch. 8.1.
[65] Une exigence correspondante a été prévue dans l'appel d'offres OMC 20007; cf. catalogue des exigences, p. 8 (ST04).

dans le contrat où le service est effectivement exploité (y compris les prestations de support), qui a accès aux données et à partir de quel endroit (cf. annexes C et D). Le traitement des données dans un lieu indéfini est inacceptable.

1.7 Accès des autorités à l'étranger

Si des données de la Confédération se trouvent à l'étranger, il est possible qu'elles soient demandées par des autorités étrangères à des prestataires de services (plutôt qu'à la Confédération en tant que maître des données, par la voie de l'entraide judiciaire). Trois scénarios d'accès des autorités (et bases juridiques correspondantes) peuvent alors se présenter:

- procédures judiciaires,
- sécurité nationale ou prévention de la criminalité (en particulier terrorisme), et
- surveillance des services de renseignement à l'étranger[66].

Dans les trois cas, il est possible que des autorités étrangères accèdent à des données de la Confédération de manière licite en vertu de leur droit, mais en violation du droit suisse et des accords contractuels conclus avec les prestataires de services[67]. Il convient alors de se demander si l'ordre juridique d'un pays de destination comporte des risques particuliers, par exemple parce que les garanties procédurales sont insuffisantes ou que l'exercice des droits est jugé particulièrement difficile.

D'une manière générale, le principe d'immunité des États prévu par le droit international permet une protection particulière en ce qui concerne l'accès d'États étrangers aux données des autorités d'un autre État. Il convient toutefois de vérifier s'il s'applique dans le cas concret[68].

Dans la mesure où les accès des autorités étrangères sont compatibles avec le droit suisse de la protection des données et les principes constitutionnels suisses, on peut considérer qu'il n'est pas nécessaire de prendre des mesures spécifiques[69]. Si des incertitudes subsistent à cet égard, une analyse s'impose[70] et il faut examiner comment une utilisation des services nuagiques conforme au droit peut quand même être garantie par des mesures de protection juridiques, techniques et organisationnelles appropriées (cf. annexe C).

Ces accès ne peuvent être totalement exclus dans aucun des trois scénarios[71]:

- *Procédures judiciaires :* dans le cadre de procédures judiciaires, il est souvent prévu[72] que les personnes qui détiennent ou contrôlent des données doivent les remettre aux autorités nationales sous certaines conditions; en outre, les autorités nationales ont généralement la possibilité de saisir des données ou du matériel informatique. La convention du Conseil de l'Europe sur la cybercriminalité (RS *0.311.43*)[73] (comme le droit en vigueur en Suisse[74]), entre autres, le prévoit. En règle générale, des garanties procédurales protègent les données, notamment lorsqu'il s'agit de données d'autorités d'autres États.

- *Finalités préventives, notamment lutte contre le terrorisme :* la collecte discrète de données stockées chez des fournisseurs de services de communication (*at rest mass surveillance*, par exemple pour les États-Unis FISA, section 702[75]) est typique de certaines bases juridiques créées ces dernières années, notamment à des fins de lutte contre le terrorisme. Celle-ci a généralement lieu à l'insu des personnes concernées et, le cas échéant, à l'insu du « maître des données ». Toutefois, leurs droits peuvent être exercés, du moins en partie, par le fournisseur de services nuagiques. Dans certains cas, ce risque devra faire l'objet d'une pondération particulière (processus d'audit visant à réduire les activités menées par des services de renseignement).

---

[66] Cf. CNA, réponse à la prise de position du PFPDT concernant M365, p. 3 s. et 7 s., avec références.
[67] Si un tel cas se produit et qu'il a été convenu que le droit suisse s'applique à l'utilisation du nuage, il y a conflit de lois. Le fournisseur de services nuagiques viole le contrat, ce qui peut avoir des conséquences (par ex. une peine conventionnelle).
[68] Le DFAE (DDIP) examine actuellement s'il est possible de parvenir à une compréhension commune du rôle de l'immunité des États dans le domaine des données des autorités avec les États pertinents. Si tel est le cas, les données de l'administration fédérale et d'autres services de l'administration publique en Suisse seront particulièrement protégées contre l'accès d'autres États en vertu du droit international.
[69] Sont notamment visés ici les principes constitutionnels suivants: le principe de légalité (art. 5 Cst.), le principe de proportionnalité (art. 5 al. 2, Cst. et. 4, al. 2, LPD) ou la garantie des voies de droit et l'accès à un tribunal impartial (art. 29 ss Cst. et 15 LPD).
[70] DAVID ROSENTHAL a développé un outil d'analyse structuré qui peut être considéré comme une « bonne pratique" : https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx
[71] Pour une présentation des différentes formes, voir ROSENTHAL, FAQ n° 28.
[72] Cf. en particulier l'art. 18, al. 1, de la convention sur la cybercriminalité et le Stored Communications Act américain.
[73] Cf. art. 18, al. 1, de la convention sur la cybercriminalité; entrée en vigueur pour la Suisse le 1er janvier 2012; mais aussi, par exemple, le Stored Communications Act américain.
[74] Cf. également LAUX/HOFFMANN sur la situation juridique de l'accès des autorités en Suisse, ch. 120 ss.
[75] La Suisse dispose également de bases légales qui permettent la collecte secrète de données, cf. aujourd'hui notamment les art. 26, al. 2, et 33 de la loi sur le renseignement ; RS **121**.

- *Exploration de communications étrangères (radio, réseau câblé) et autres activités de renseignement :* de nombreux États[76] disposent de bases légales permettant d'explorer ou d'écouter des communications qui ont lieu à l'étranger entre des personnes cibles de nationalité étrangère. Toute transmission de données entre l'utilisateur et le fournisseur de services nuagiques est potentiellement exposée à ce risque, sauf s'il peut être garanti qu'elle a lieu uniquement sur le territoire national. L'accès *ciblé* aux données par des services de renseignement depuis l'étranger est en principe possible partout, même lorsque les données sont traitées dans des centres de calcul propres particulièrement sécurisés[77].

La situation juridique concernant l'UE, les États-Unis et la Chine est brièvement analysée ci-après. Ces exemples ont été choisis parce qu'il s'agit des pays où se trouvent les sièges des sociétés mères ou des filiales des principaux fournisseurs hyperscalaires et d'autre part parce que la question de l'accès des autorités se pose tout particulièrement dans ces juridictions en raison de leurs réglementations particulières, qui diffèrent du droit suisse et de « l'acquis » européen. Les filiales européennes de sociétés ayant leur siège dans ces États ne sont pas directement ou obligatoirement soumises à ces règles. Des accords contractuels spécifiques doivent être prévus, le cas échéant[78].

Dans la mesure où il faut s'attendre à ce que des risques résiduels subsistent, il convient, selon le point de vue défendu ici, de les ramener à un niveau acceptable par des mesures appropriées.

Dans ce contexte, il convient de noter que le Préposé fédéral à la protection des données et à la transparence défend un autre point de vue juridique. Il se fonde sur une pratique stricte récemment établie par certaines autorités de protection des données de l'UE, qui se réfèrent à la jurisprudence de la Cour de justice de l'UE[79]. Il doute notamment que l'actuelle, comme la nouvelle, législation fédérale en matière de protection des données permette une approche basée sur les risques lorsqu'il s'agit d'évaluer la légalité du traitement de données d'autorités suisses, par des sous-traitants liés à un État étranger dont la législation et la pratique des autorités pourraient entraîner un accès non transparent aux données. Selon l'opinion défendue ici - fondée sur la conception solidement étayée de plusieurs juristes spécialisés[80] - il existe cependant des arguments juridiques et pratiques convaincants qui plaident pour une position plus nuancée[81]. En particulier, il ne ressort pas des dispositions pertinentes du droit suisse de la protection des données qu'une approche basée sur les risques serait inadmissible pour les autorités en cas de sous-traitance ou de communication des données à l'étranger[82].

1.7.1 Situation juridique en relation avec les membres de l'UE

La transmission de données personnelles de la Suisse à des destinataires domiciliés dans des États de l'UE ne pose pas de problème du point de vue de la protection des données. Le règlement général de l'UE sur la protection des données (RGPD) correspond à un standard sur lequel se fondent également les règles de la nLPD. Selon la liste des pays du PFPDT, les États membres de l'UE disposent d'une législation adéquate en matière de protection des données.

Même dans les pays de l'UE (à l'exception de l'Irlande, tous les États membres ont adhéré à la convention sur la cybercriminalité [83]), le risque existe que les autorités accèdent à des données dans le cadre de procédures judiciaires, à des fins de prévention et dans le cadre de mesures de surveillance à l'étranger. On peut néanmoins considérer qu'il n'existe pas de risques juridiques particuliers dans les pays de l'UE et que des garanties procédurales suffisantes existent en ce qui concerne les accès des autorités. Le cas échéant, il convient d'examiner s'il existe des risques politiques ou autres (voir annexe C).

---

[76] La Suisse dispose également d'une base légale pour l'exploration radio, cf. art. 38 ss de la loi sur le renseignement.
[77] Voir également ROSENTHAL, FAQ n° 34. L'espionnage ciblé par les services de renseignement n'est pas exclu, même avec des solutions de haute sécurité sur site ; voir par exemple NICOLE PERLROTH, The Cyber Weapons Arms Race, Londres 2021, p. 320 ss.
[78] Cf.. CNA, réponse à la prise de position du PFPDT concernant M365, p. 7 s., avec références.
[79] La position critique du PFPDT à l'égard de l'approche basée sur les risques en ce qui concerne la communication de données à l'étranger est exposée ici; communiqué du 13 juin 2022 Externalisation de données personnelles par la Suva vers un cloud de Microsoft.
[80] CHRISTIAN LAUX / ALEXANDER HOFFMANN, DAVID ROSENTHAL, DAVID VASELLA.
[81] La CNA (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2022/Antwort.%20Suva,%20Luzern%2020220513.%20Risikobeurteilung%20Projekt%20Digital%20Workplace%20_M365_.pdf.download.pdf/Antwort.%20Suva,%20Luzern%2020220513.%20Risikobeurteilung%20Projekt%20Digital%20Workplace%20_M365_.pdf et la doctrine ont répliqué à ses objections, cf. en particulier DANIEL VASELLA, EDÖB, Zweifel am risikobasierten Ansatz, datenrecht.ch 13.6.2022 (https://datenrecht.ch/edoeb-zweifel-am-risikobasierten-ansatz/). Le présent rapport s'aligne sur la position défendue notamment par la CNA.. Pour l'évaluation des risques, voir la méthodologie décrite dans ROSENTHAL, Mit Berufsgeheimnissen in die Cloud ainsi que la FAQ récemment publiée à ce sujet, notamment les n^{os} 28 ss. Voir également CHRISTIAN LAUX / ALEXANDER HOFFMANN, Rechtmässigkeit von Public Cloud Services. Avis de droit, notamment ch. 2015. Comme il n'existe actuellement aucune jurisprudence en Suisse concernant l'approvisionnement infonuagique des autorités, un tribunal pourrait apprécier la situation différemment.
[82] Outre les experts cités, la prise de position de privatim ne considère pas non plus, pour autant que l'on puisse en juger, qu'une approche basée sur les risques serait inadmissible. Voir également la FAQ concernant l'utilisation des technologies nuagiques(www.vud.ch/view/data/2124/Div. Dokumente/220826_VUD_FAQ zum Einsatz von Cloud.pdf), qui reconnaît explicitement l'approche basée sur les risques.
[83] Voir l'aperçu ici : https://www.coe.int/fr/web/cybercrime/the-budapest-convention (8.8.2022).

1.7.2 Situation juridique en relation avec les États-Unis

Pour les États-Unis, la question se pose en raison de certains programmes de surveillance des services de renseignement[84] (« accès des services secrets ») et de la possibilité, prévue par le CLOUD Act, pour les autorités de poursuite pénale d'accéder aux données stockées chez le fournisseur de services nuagiques sans passer par une procédure d'entraide judiciaire (accès des autorités judiciaires). L'US CLOUD Act et le FISA sont souvent perçus comme des risques importants[85]. Ces lois permettent dans certains cas aux autorités américaines d'accéder à des données, même si ces données sont traitées ou hébergées en dehors des États-Unis, notamment par des sociétés sises aux États-Unis ou ayant d'autres liens juridiques avec les États-Unis (*incorporated in the United States*)[86].

En principe, les filiales européennes de sociétés américaines sont également soumises à ces dispositions (mais des exceptions s'appliquent dans de nombreux cas de figure[87]). Toutefois, une injonction de production des autorités de poursuite pénale américaines qui leur est directement adressée ne peut pas être exécutée par la contrainte pénale en dehors du territoire américain. Il est donc fort probable que les autorités de poursuite pénale américaines adresseront leurs injonctions de production aux sociétés mères sises aux États-Unis. Dans la pratique, la divulgation des données de la filiale européenne à la société mère américaine dépendra en partie de la pression économique que cette dernière exerce ou peut exercer sur sa filiale. L'avenir dira dans quelle mesure des accords contractuels entre le client et la filiale européenne peuvent apporter une protection efficace contre la divulgation ; les accords contractuels doivent donc être combinés avec d'autres mécanismes de protection.

Procédures judiciaires: CLOUD Act

Les mesures prises par les autorités en vertu du US-CLOUD Act sont soumises à certaines conditions : seules les autorités de poursuite pénale peuvent agir sur la base du CLOUD Act pour poursuivre des infractions graves. Les données ne doivent être communiquées par les fournisseurs de services nuagiques que s'ils ont un contrôle effectif ou juridique sur elles[88]. Ces notions sont toutefois issues du droit américain et utilisées par les autorités de poursuite pénale américaines conformément à la compréhension américaine. Les fournisseurs de services nuagiques peuvent contester les mesures devant un tribunal américain ; des garanties procédurales existent[89]. Il n'existe pas de protection juridique en Suisse ; il est douteux que la protection juridique qui n'est prévue qu'à l'étranger soit compatible avec le droit supérieur de la Suisse (en particulier avec la Constitution)[90].

Le risque d'accès par les autorités peut toutefois être considérablement réduit si des mesures techniques sont prises pour empêcher le fournisseur de services nuagiques d'accéder aux données. Les fournisseurs de services nuagiques ne peuvent pas être contraints de décrypter les données si seuls les utilisateurs disposent des clefs.

La communication de données liées au contenu dans le cadre de telles procédures est très rare[91].

Finalités préventives et surveillance à l'étranger (FISA et E. O. 12.333)

Le FISA permet à certaines autorités d'acquérir des informations de l'étranger. Selon la section 702, l'*Attorney General* et le *Director of National Intelligence* peuvent autoriser la collecte d'informations sur certaines personnes si l'on peut supposer qu'elles ne se trouvent pas aux États-Unis. Dans ces cas, les fournisseurs de services de communication sont tenus de rechercher les données dont ils disposent[92].

Par contre, il n'existe que des garanties procédurales limitées pour les accès aux données selon le FISA. Les données provenant d'autorités étrangères peuvent bénéficier d'une certaine protection, mais celle-ci ne peut pas toujours satisfaire aux exigences qui découlent du droit suisse, notamment

[84] Cf. arrêt Schrems II de la CJUE: https://curia.europa.eu/jcms/jcms/P_64268/fr/ et FAQ concernant l'utilisation des technologies nuagiques (www.vud.ch/view/data/2124/Div. Dokumente/220826_VUD_FAQ zum Einsatz von Cloud.pdf), qui reconnaissent explicitement l'approche basée sur les risques.
[85] ROTH, Cloud-basierte Dienstleistungen im Licht der DSGVO, p. 68; cf. aussi BRAUNECK Europa-Cloud: Zwingt der US CLOUD Act EU-Unternehmen zur EU-rechtswidrigen Datenherausgabe? Oder ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act
[86] Cf. Office fédéral de la justice, rapport sur l'US CLOUD Act, p. 6, avec référence à un document du Département américain de la justice.
[87] Cf. ROSENTHAL, FAQ n° 32, 35 et 36.
[88] ROSENTHAL, FAQ n° 35. Selon le rapport de l'Office fédéral de la justice, il est essentiel que le fournisseur de services infonuagiques ne puisse pas accéder à la clef; cf.Office fédéral de la justice, op. cit.
[89] Cf. par exemple. Nouvelles mesures pour protéger vos données – Microsoft Suisse Espace presse; etROSENTHAL, Mit Berufsgeheimnissen in die Cloud, p. 40 FAQ n° 29. Une description détaillée des processus se trouve chez LAUX/HOFFMANN, p. 42 ss.
[90] Voir Office fédéral de la justice, rapport sur le US CLOUD Act, p. 29 ss et 38 s.
[91] Cf. par exemple LAUX/HOFFMANN Rz. 208 ff. Law Enforcement Request Report | Microsoft CSR; cf. ROSENTHAL, Mit Berufsgeheimnissen in die Cloud, p. 33 s.
[92] Pour plus de détails, voir ROSENTHAL, FAQ n° 29.

en matière de protection des données[93]. En outre, la transparence n'est pas garantie dans la mesure où les fournisseurs de services nuagiques ne sont pas autorisés à fournir des informations sur le fait qu'une autorité demande l'accès aux données (*gag order*). Les fournisseurs de services nuagiques disposent de moyens juridiques pour contester les ordres de surveillance[94].

Il existe cependant des conditions qui doivent être remplies (notamment en ce qui concerne le statut du fournisseur de services nuagiques en tant que fournisseur de services de communication et le fait que des *US Persons* peuvent être concernées par les mesures de surveillance) et qui peuvent faire l'objet d'une appréciation basée sur les risques[95]. Ici aussi, il est possible de prendre des mesures techniques (cryptage suffisamment fort) pour empêcher l'accès au contenu des données en texte clair[96].

L'E. O. 12.333 est axé sur l'acquisition de données pendant leur transmission *(données en transit*). Les conditions sont définies de manière similaire à la section 702 FISA. Si ces données sont cryptées de manière suffisamment forte lors de leur transmission et que les fournisseurs de services de communication impliqués n'ont pas accès aux clefs, il n'y a en principe pas de risque accru[97].

Conclusions

Il existe des indications dans le droit américain selon lesquelles, en ce qui concerne l'accès aux données par les autorités américaines, les données stockées par une autorité étrangère (p. ex. suisse) auprès d'un fournisseur de services nuagiques soumis aux lois américaines pertinentes bénéficient d'une protection particulière contre les accès aux données sur la base de l'US CLOUD Act ;il existe en outre des mécanismes procéduraux correspondants (par ex. selon les principes de la Common-Law Comity Analysis ou du US Foreign Sovereign Immunities Act)[98]. Les tribunaux américains décident de l'application de ces règles dans le cadre des Federal Rules of Criminal Procedure; il n'y a donc pas de garantie absolue que la souveraineté suisse est protégée. Dans ce cadre, l'autorité fédérale suisse doit s'assurer que, dans le cas d'une demande des autorités américaines, le fournisseur de services nuagiques signale dans la procédure que son client est un État étranger qui revendique sa souveraineté[99].

Sur la base de la situation juridique actuelle, il convient d'évaluer au cas par cas si une combinaison des conditions prévues dans les dispositions et mécanismes pertinents du droit américain, des accords contractuels (en particulier l'obligation du fournisseur de contester les divulgations par voie judiciaire aux États-Unis) et des mesures de protection techniques, permet de limiter à un risque acceptable d'un point de vue juridique un accès aux données non conforme au droit suisse, même dans le cas des accès selon le FISA et l'E. O. 12.333. Il faut donc toujours procéder à un examen adapté aux circonstances concrètes.

1.7.3 Situation juridique en relation avec la Chine

S'agissant de la Chine, il est difficile d'évaluer l'ampleur des risques d'accès par les autorités. On ne peut exclure que les autorités chinoises puissent accéder à des données stockées en Chine ou à l'étranger par des fournisseurs de services nuagiques chinois, ou les bloquer, sans garanties procédurales fiables[100]. Le grand nombre de bases légales applicables à l'accès aux données complique également toute évaluation[101].

Le routage de « données en transit » par la Chine pourrait en outre comporter des risques particuliers concernant la disponibilité et l'intégrité des données, notamment en raison des particularités de la connexion du réseau intérieur chinois à l'Internet mondial[102].

---

[93] Fait actuellement l'objet de clarifications au sein du DFAE. Les données dans le contexte diplomatique et consulaire sont protégées par le droit international.
[94] ROSENTHAL, FAQ, n° 29, notamment *in fine*.
[95] Cf. VASELLA; a.A. privatim, ch. 2.2. Détaillé avec différentes distinctions de cas ROSENTHAL, FAQ, n° 29.
[96] ROSENTHAL, FAQ n°s 32 et 35.
[97] ROSENTHAL, FAQ n° 29.
[98] Cf. LAUX/HOFFMANN, ch. 205 s., 215 et CNA, p. 3 s.
[99] Il faut toutefois tenir compte du fait que la décision concernant d'éventuelles immunités relève uniquement des autorités américaines, sans aucune participation de la Suisse jusqu'à présent. Des clarifications sont en cours à ce sujet entre le DFJP et le DFAE et les autorités américaines compétentes. Les clarifications approfondies en cours visent également à déterminer dans quelle mesure l'immunité des États prévue par le droit international garantit une protection particulière aux données des autorités à l'instar des données des organisations internationales et des représentations diplomatiques et consulaires.
[100] Voir également les références chez ROSENTHAL, FAQ, n° 28.
[101] Voir par exemple la liste pour l'exemple de la Chine dans ROSENTHAL, EU-SCC Transfer Impact Assessment ; https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx (7 août 2022).
[102] Cf. par exemple Jonathan E. HILLMANN, The Digital Silk Road, Londres 2021, p. 153.

En raison de la loi sur la sécurité des données nationale, les autorités chinoises doivent impérativement avoir accès aux données ; il se pourrait en outre que les données hébergées en Chine ne puissent plus, le cas échéant, être retransférées vers la Suisse ou d'autres pays[103]; par ailleurs, le cryptage des données est interdit, dans la mesure où les autorités chinoises n'y auraient plus accès. Au surplus, la législation chinoise interdit l'utilisation de connexions sécurisées par VPN[104].

La transmission de données personnelles en Chine implique donc en soi des risques considérables et difficilement évaluables qui la rendent difficilement compatible avec les exigences du droit suisse de la protection des données et d'autres exigences légales.

Toute transmission de données personnelles à une filiale d'une société chinoise doit être examinée avec soin afin de déterminer si et dans quelles conditions la société mère ou les autorités chinoises peuvent avoir accès aux données contrôlées par la filiale.

1.7.4 Autres risques (politiques) généraux liés aux solutions nuagiques à l'étranger

D'autres risques (en particulier politiques) doivent être évalués dans l'optique d'une solution nuagique à l'étranger et, dans la mesure du possible, compensés par des règles contractuelles appropriées : il s'agit en particulier des risques suivants (voir également l'annexe C):

- modification de la situation juridique dans l'État concerné, notamment en ce qui concerne l'accès des autorités aux données : définir de manière appropriée la durée du contrat et, le cas échéant, définir des « clauses de sortie »
- délocalisations dans d'autres pays et modifications du cadre juridique qui en résultent : convenir de garanties contractuelles concernant les sites d'hébergement;
- pression politique sur les fournisseurs de services nuagiques en vue de la communication de données ou de clefs ou de la mise à disposition de clefs supplémentaires (*backdoors*) : examen préalable et observation de l'évolution politique.

Il pourrait également être nécessaire d'examiner si des raisons de « politique de souveraineté » pourraient éventuellement conduire à ne pas épuiser la marge de manœuvre juridique existante s'agissant de l'externalisation dans le nuage de certains ensembles de données.

1.8 Droits des personnes concernées

1.8.1 Principe

Les personnes dont les données sont traitées jouissent de droits individuels en vertu de la loi sur la protection des données. En font notamment partie le droit d'accès (art. 25 nLPD) et le droit d'exiger que l'organe responsable s'abstienne de procéder à un traitement illicite ou efface les données traitées de manière illicite (art. 41 nLPD).

Le droit d'accès porte sur les données personnelles traitées en tant que telles, la finalité du traitement, la durée de conservation des données personnelles, les informations disponibles sur l'origine des données personnelles dans la mesure où elles n'ont pas été collectées auprès de la personne concernée, le cas échéant, l'existence d'une décision individuelle automatisée ainsi que la logique sur laquelle se base la décision, le cas échéant, les destinataires ou les catégories de destinataires auxquels les données personnelles sont communiquées (art. 25, al. 2, nLPD). L'unité administrative responsable du traitement est responsable de la communication des informations. Elle doit veiller à ce que le droit d'accès puisse être garanti. Il en va de même pour le droit à la remise ou à la transmission de données conformément à l'art. 28 nLPD.

En vertu de l'art. 41, al. 2, let. a, nLPD, quiconque a un intérêt digne de protection peut exiger que l'unité administrative rectifie, efface ou détruise des données personnelles si ces données sont traitées de manière illicite. L'intérêt est digne de protection lorsque la personne est concernée. C'est toujours le cas pour ses propres données personnelles. Dans certaines conditions (notamment lorsque l'exactitude des données est contestée et que ni leur exactitude ni leur inexactitude ne peuvent être établies), le traitement doit être limité (art. 41, al. 3, let. a, nLPD).

[103] Cf. par exemple Steve DICKINSON, China's new cybersecurity law : no place to hide, 11 octobre 2020 ; https://harrisbricken.com/chinalawblog/china-cybersecurity-no-place-to-hide/ (14 janvier 2022).
[104] Cf. par exemple NZZ, China baut weltweit ersten «Freihafen für Daten», 21 janvier 2022, p. 23.

1.8.2 Dans le contexte du nuage

L'exercice des droits doit également être garanti lorsque les données concernées sont traitées dans le nuage. En ce qui concerne l'externalisation dans le nuage, il faut donc s'assurer que les données peuvent être effacées (ou éventuellement détruites) de manière fiable. Le cas échéant, le fournisseur de services nuagiques doit être explicitement tenu par contrat de garantir l'effacement irréversible des données.

2 Secret de fonction

2.1 Remarques générales

Le secret de fonction poursuit principalement deux objectifs, d'une part protéger le citoyen et ses secrets et d'autre part l'administration afin qu'elle puisse travailler librement. Il est inscrit à l'art. 320 CP pour les employés de l'administration fédérale et rappelé à l'art. 22 de la loi sur le personnel de la Confédération (LPers, RS *172.220.1*). Pour les employés de l'administration fédérale, l'obligation de garder le secret est également fixée dans des dispositions sectorielles du droit fédéral (par ex. art. 61 ss de la loi sur les produits thérapeutiques [RS *812.21*]). L'accent est mis ici sur la violation du secret de fonction sanctionné par l'art. 320 CP, qui fixe les conséquences pénales[105].

La loi du 17 décembre 2004 sur la transparence (LTrans ; RS *152.3*) reflète la notion de secret de fonction et limite la « portée » du secret de fonction[106]. Depuis que le principe de transparence a été mis en œuvre dans l'administration fédérale, le cercle des informations qui sont (ou peuvent être) soumises au secret de fonction s'est réduit. Selon la LTrans, il y a obligation de garder le secret:

- si le secret prévu par une loi spéciale (art. 4 LTans), ou
- s'il y a une exception au principe de transparence (art. 3, 7 et 8 LTrans)[107].

Une éventuelle classification des informations n'implique pas qu'elles sont soumises au secret de fonction. Cela vaut en particulier pour les informations qui sont classifiées « INTERNE » (cf. art. 13, al. 3, OPrI et ch. 5 ci-après).

2.2 Violation du secret de fonction (art. 320 CP)

2.2.1 Éléments constitutifs de l'infraction

L'incertitude juridique quant à savoir si le traitement de données soumises au secret de fonction par un prestataire de services externe constitue une violation du secret de fonction est aujourd'hui considérable. Pour tenir compte de cette incertitude, la punissabilité de la violation du secret de fonction est désormais étendue aux auxiliaires (par analogie avec les secrets professionnels selon l'art. 321 CP). Le nouvel art. 320 CP, adopté avec la loi sur la sécurité de l'information (cf. ci-après ch. 4.2), doit être mis en vigueur de manière anticipée le 1er janvier 2023. L'analyse qui suit se fonde donc sur le nouveau droit.
En vertu de l'art. 320, ch. 1, nCP est punissable « quiconque révèle un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il a eu connaissance à raison de sa charge ou de son emploi ou en tant qu'auxiliaire d'une autorité ou d'un fonctionnaire ».
Les conditions suivantes doivent être remplies de manière cumulative pour que les éléments constitutifs de la violation du secret de fonction soient réunis:

- L'auteur peut être un fonctionnaire au sens de l'art. 110, al. 3, CP[108] ou l'auxiliaire d'un fonctionnaire. La définition légale couvre les fonctionnaires institutionnels et fonctionnels[109].

[105] Il convient de mentionner ici que d'autres dispositions pénales peuvent être pertinentes, en plus de l'art. 320 CP, par exemple l'art. 267 CP (trahison diplomatique). Toutefois, comme ce dernier n'est plus appliqué depuis des décennies, il ne sera pas examiné ici de manière plus approfondie.
[106] Voir également à propos de cette délimitation OFJ/PFPDT : FAQ: mise en œuvre du principe de transparence (admin.ch)), ch. 1.1.2 et 1.1.3 (20 juin 2022).

[108] Par fonctionnaires au sens de l'art. 110, al. 3, CP, on entend les fonctionnaires et les employés d'une administration publique et de la justice ainsi que les personnes qui occupent une fonction publique à titre provisoire, ou qui sont employés à titre provisoire par une administration publique ou la justice ou encore qui exercent une fonction publique temporaire.
[109] Cela signifie que la forme juridique sous laquelle une personne travaille pour la collectivité n'a pas d'importance. La relation peut être de droit public ou de droit privé. C'est la fonction des activités qui est déterminante. Si celles-ci consistent en l'accomplissement de tâches publiques, elles sont officielles et les personnes qui les exercent sont des fonctionnaires au sens du droit pénal (ATF 135 IV 198, consid. 3.3).

- Sont secrets tous les faits qui ne sont ni de notoriété publique, ni généralement accessibles (secret relatif), pour lesquels il existe un intérêt légitime au maintien du secret et que le détenteur du secret veut garder confidentiels (secret matériel)[110].
- L'acte consiste en la divulgation du secret de fonction. Divulguer signifie rendre le secret accessible à un tiers auquel cette information n'est pas destinée[111].
- Pour être complet, il convient de mentionner ici que la réalisation de l'élément constitutif de l'infraction présuppose que la divulgation du secret est intentionnelle, le dol éventuel étant suffisant.

2.2.2 Évaluation des éléments constitutifs de l'infraction dans le contexte du nuage

2.2.2.1 Caractère secret des données transmises à un fournisseur de services nuagiques

La communication de données à un fournisseur de services nuagiques est licite, car il est tenu au secret en vertu de l'art. 320, ch. 1, nCP. Les art. 10*a* LPD et 11 OTNI prévoient tous deux expressément le traitement des données par des tiers sous certaines conditions. L'art. 10*a* LPD réserve toutefois les obligations légales ou contractuelles de garder le secret. Celles-ci, pas plus que le secret de fonction, n'excluent toutefois pas le traitement de données personnelles par des tiers[112]. L'art. 320 nCP n'interdit donc pas de sous-traiter les données personnelles au sens de l'art. 9 nLPD[113]. Avant de recourir à une solution nuagique (ou à un autre modèle d'externalisation), il faut dans tous les cas analyser si les données à externaliser sont accessibles conformément aux règles de la LTrans ou en vertu d'autres dispositions[114] ou si elles sont soumises à des exigences particulières en matière de confidentialité en raison de bases légales spécifiques (analyse des besoins de protection et des risques, voir ch. 3.2). Les mesures de protection appropriées, en particulier les mesures techniques et organisationnelles de protection des données et de l'information (art. 11 OTNI) seront définies sur cette base.

2.2.2.2 Consultation des informations par le fournisseur de services nuagiques ou des tiers (« divulgation »)

L'accès du fournisseur de services nuagiques à des données secrètes doit, dans le cadre d'une externalisation en nuage, être limité de manière appropriée, voire exclu par des mesures contractuelles, organisationnelles et techniques. La mesure dans laquelle le fournisseur de services nuagiques (ou les collaborateurs ou « sous-traitants » mandatés par lui) doit pouvoir consulter le contenu des données pour exécuter ses tâches ou peut (théoriquement) le faire dans ce cadre, dépend notamment du modèle de service choisi. En règle générale, le risque d'une consultation devrait être plus faible pour les modèles IaaS et PaaS (parce que les données sont traitées en grande partie au moyen de logiciels définis et exploités par l'utilisateur du nuage) que pour les modèles SaaS.

Le fournisseur de services nuagiques peut accéder aux données dans certains cas, car il contrôle le système sur lequel se trouvent les données et aurait donc les possibilités techniques nécessaires, au moins pendant certaines phases du traitement (données en cours d'utilisation). Il existe toutefois de nombreuses mesures permettant d'empêcher l'accès ou de le rendre beaucoup plus difficile dans les infrastructures en nuage. Si l'accès aux données est indispensable, il doit être limité au strict nécessaire (par ex. pour le support, dans certains cas et sous certaines conditions[115]). Si les mesures nécessaires ont été prises adéquatement, notamment en cas de cryptage ou de pseudonymisation des données, il est possible d'éviter dans une large mesure que des données soient divulguées.[116]

L'accès aux données par d'autres tiers (par ex. des autorités étrangères) doit également être réduit de manière adéquate par des mesures appropriées et adaptées aux risques[117].

[110] ATF 127 IV 122 ; BSK StGB-Oberholzer, art. 320 n. 8.
[111] BSK StGB-Oberholzer, art. 320 n. 9.
[112] BÜHLER/RAMPINI, in : MAURER-LAMBROU/BLECHTA (éd.), Commentaire LPD et LTrans, art. 10*a* LPD, n. 1.
[113] GA WIDMER, S.20; RUDIN, Bearbeiten im Auftrag, p. 83 in: Praxiskommentar IDG Bâle-Ville.
[114] Cf. à l'avenir notamment l'art. 10 du projet de loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (FF 2022 805). https://www.fedlex.admin.ch/eli/fga/2022/805/fr) concernant les données ouvertes.
[115] Par exemple, si le mandant a autorisé l'accès dans le cas d'espèce.
[116] SCHWARZENEGGER, THOUVENIN, STILLER, GEORGE, Revue de l'avocat 2019, p. 28.
[117] Voir l'avis du ministère public de BS sur le projet M365 du point de vue du droit pénal, du 19 avril 2020.

2.2.2.3 Déliement du secret de fonction

Selon l'art. 320, ch. 2, CP, l'auteur n'est pas punissable s'il a révélé le secret avec le consentement écrit de l'autorité supérieure. Ce consentement est adapté à des cas concrets et ne doit pas être utilisé abusivement comme un consentement global.

2.2.2.4 Statut d'auxiliaire du fournisseur de services nuagiques

La réglementation contractuelle entre l'administration fédérale et le fournisseur de services nuagiques est un contrat de mandat au sens du droit privé. Conformément aux bases légales des solutions d'externalisation exposées ci-dessus, le fournisseur de services nuagiques n'est pas un tiers non autorisé au sens de l'art. 320 nCP, mais un auxiliaire.

2.3 Conclusion

Conformément à ce qui précède, l'externalisation des données dans le nuage ne constitue pas une violation du secret de fonction au sens de l'art. 320 nCP, pour autant que les prescriptions de l'art. 11 OTNI soient respectées. Les collaborateurs de l'administration fédérale ne sont donc en principe pas punissables pour violation du secret de fonction lorsqu'ils transfèrent des données dans le nuage.

Il peut y avoir violation du secret de fonction notamment si le fournisseur de services nuagiques met les données à la disposition d'un tiers sans autorisation. Différents moyens sont disponibles pour l'éviter. Les données peuvent notamment être cryptées ou pseudonymisées (cf. ch. 2.2.1) ou tokenisées[118]. Le fournisseur de services nuagiques devrait alors contourner des mesures techniques et violerait dans tous les cas ses obligations contractuelles (et éventuellement d'autres dispositions pénales, par ex. l'art. 271 CP [actes exécutés sans droit pour un État étranger] ou les art. 272 à 274 CP [services de renseignements politiques, économiques ou militaires]).

Comme le fournisseur de services nuagiques est généralement sis à l'étranger, la question de l'application du droit pénal suisse en cas de violation du secret de fonction par un collaborateur d'une entreprise étrangère se pose naturellement. Selon le pays, la poursuite pénale pourrait donc être difficile, voire impossible.

Des questions très délicates pourraient se poser en cas d'externalisation lorsqu'un État dispose de larges possibilités d'accès (en fait et en droit) aux données d'entreprises situées dans sa sphère d'influence et que l'administration le sait.

3 Ordonnance sur les cyberrisques (OPCy)

L'ordonnance du Conseil fédéral sur la protection contre les cyberrisques dans l'administration fédérale (OPCy) traite spécifiquement des cyberrisques et de la sécurité informatique de la Confédération. Elle sera abrogée lorsque l'OSI entrera en vigueur, probablement en juillet 2023.

En ce qui concerne les projets nuagiques, ce sont surtout les procédures de sécurité applicables aux objets informatiques à protéger qui sont pertinentes (art. 14*b* ss OPCy).

3.1 Objets informatiques à protéger (art. 3, let. h, OPCy)

Selon l'art. 3, let. h, OPCy, les objets informatiques à protéger sont les applications, services, systèmes, réseaux, fichiers de données, infrastructures et produits relevant de l'informatique. Plusieurs objets identiques ou connexes peuvent être regroupés en un seul objet informatique à protéger. Cela signifie que les données qui sont transférées dans un nuage peuvent être regroupées en un objet informatique à protéger et faire l'objet d'une seule procédure de sécurité, ce qui permet de gagner du temps. Il ressort donc de l'art. 3, let. h, OPCy que, outre les éléments informatiques traditionnels (tels que les composants de réseau actifs, les serveurs et autres produits informatiques), les services et notamment les fichiers de données sont également des objets informatiques à protéger. Tous les fichiers qui, sous quelque forme que ce soit, sont générés, gérés, externalisés par l 'administration fédérale ou dont la responsabilité lui incombe doivent donc être vérifiés sous l'angle de leur conformité à l'OPCy. On peut en déduire que tous les fichiers hébergés par des fournisseurs de services nuagiques nationaux ou étrangers sont soumis à l'OPCy.

[118] Cf. également CNA, p. 8.

Conformément aux art. 14*b* ss OPCy, tous les objets informatiques à protéger doivent être régulièrement contrôlés au moyen d'une procédure de sécurité.

3.2 Procédures de sécurités visées au chapitre 3*a*

Les procédures de sécurité définissent les étapes du processus qui doivent être mises en œuvre pour garantir la sécurité de l'information. Conformément à l'art. 14*b*, al. 1, OPCy, les unités administratives s'assurent qu'une analyse actuelle des besoins de protection est disponible pour tous les objets informatiques à protéger. Les projets informatiques doivent faire l'objet d'une telle analyse avant d'être validés. L'analyse des besoins de protection aide à déterminer quelles données sont traitées avec l'objet informatique à protéger. Les exigences qui doivent être remplies sont ensuite vérifiées sur cette base. L'art. 14*c* OPCy prévoit que les protections de base pour tous les objets informatiques à protéger doivent être mises en œuvre et documentées. L'art. 14*d* OPCy règle la procédure à suivre si l'analyse révèle des besoins de protection accrus.

S'agissant des projets nuagiques, cela signifie que les risques doivent être identifiés avant que les données puissent être transférées dans le nuage (voir à ce sujet l'annexe C). Si l'analyse révèle des besoins de protection accrus (par ex. présence de données sensibles), les unités administratives doivent définir d'autres mesures de sécurité et mettre en évidence les éventuels risques résiduels (art. 14*d*, al. 1 et 2, OPCy) ou renoncer à l'externalisation.

Pour les projets nuagiques, il faut notamment évaluer dans le cadre de l'analyse des besoins de protection si les objets à protéger sont fortement exposés à un espionnage des services de renseignement. Dans ce cas, il faut également engager un processus d'audit visant à réduire les activités menées par des services de renseignement (GRAES)[119]. Si les fournisseurs de services nuagiques sont domiciliés dans des États ou ont des liens avec des États dans lesquels les activités menées par les services de renseignement ne peuvent être exclues, cette question doit être examinée de manière approfondie[120]. Nous estimons toutefois qu'il n'y a de risque important, et donc d'obligation d'engager un GRAES, que si les données doivent être considérées comme sensibles (par ex. secrets professionnels, d'affaires ou de fabrication de tiers, autres informations personnelles délicates, données concernant la sécurité intérieure ou extérieure de la Suisse). Cette condition ne s'applique manifestement pas aux données qui sont généralement accessibles au public.

4 Dispositions concernant la protection des informations de la Confédération

L'ordonnance du 4 juillet 2007 sur la protection des informations (OPrI, RS *510.411*) sera remplacée par l'ordonnance sur la sécurité de l'information (OSI) à l'entrée en vigueur de la LSI. Le présent chapitre se concentre sur le droit en vigueur (cf. ch. 5.1). Toutefois, afin de tenir compte de la planification de projets de longue durée, les principales nouveautés de la LSI et les modifications d'autres actes découlant la LSI et qui pourraient être pertinentes pour les projets nuagiques sont présentées schématiquement au ch. 5.2.

4.1 Ordonnance sur la protection des informations (OPrI)

4.1.1 Contenu

L'OPrI règle la protection des informations de la Confédération (c'est-à-dire pour l'administration fédérale selon les art. 7 et 7*a* LOGA), de l'armée et de la protection civile (cf. art. 1, al. 1, en relation avec les art. 4 à 7 OPrI). Pour ce faire, elle règle notamment la classification et le traitement des informations (cf. prescriptions de traitement visées à l'art. 18 en relation avec l'annexe OPrI). Les règles relatives à la protection transfrontalière des informations figurent dans les accords internationaux sur la protection des informations[121] entre la Suisse et ses partenaires étrangers.

Quiconque traite des informations classifiées, en tant qu'employé de l'administration fédérale, militaire ou membre de la protection civile, organisation ou personne de droit public ou privé, ou en tant que tribunal fédéral ou cantonal, est responsable du respect des prescriptions relatives à la protection des

[119] Cf. à ce sujet: Appréciation des besoins de protection (admin.ch) https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/vorgaben/prozesse/p041/P041-Schutzbedarfsanalyse_V4-5-f.pdf.download.pdf/P041-Schutzbedarfsanalyse_V4-5-f.pdf p. 8 s. Le GRAES est couvert par la procédure de sécurité relative aux entreprises prévue par la LSI.
[120] C'est notamment le cas des externalisations visées par l'appel d'offres OMC 20007.
[121] Affaires internationales et visites.

informations (cf. art. 12, al. 1, OPrI) ; les prescriptions relatives à la protection des données personnelles prévues par la LPD s'appliquent indépendamment de l'applicabilité de l'OPrI et doivent être examinées séparément ou sont applicables parallèlement à l'OPrI.

Si des informations classifiées conformément à l'OPrI sont traitées ou créées dans un nuage, le projet doit être planifié en conséquence. Il n'existe aujourd'hui pas de disposition de droit matériel interdisant en soi l'utilisation du nuage dans l'administration fédérale pour les informations classifiées INTERNE ou CONFIDENTIEL (l'utilisation du nuage est toutefois interdite pour les informations classifiées SECRET[122]). Les dispositions suivantes s'appliquent parallèlement à l'OPrI[123]:

- directives de traitement du 18 janvier 2008 (cf. art. 18, al. 2, OPrI),
- catalogue des classifications du 26 septembre 2011.

4.1.2 Traitement des informations dignes de protection et applicabilité de l'OPrI

La direction du projet doit vérifier avant le début du projet et, si nécessaire, en cours de route, si des informations dignes de protection sont concernées et donc si l'OPrI est applicable (analyse des besoins de protection visée à l'art. 14*b* OPCy). Les méthodes courantes de gestion de projet (par ex. HERMES) le prévoient d'ailleurs explicitement.

Les considérations suivantes peuvent être utiles pour les projets nuagiques (voir également l'annexe E) :

Quiconque rédige ou publie des informations dignes de protection doit leur attribuer les échelons de classification suivants en fonction du degré de protection requis: INTERNE, CONFIDENTIEL, SECRET (cf. art. 4, al. 1, OPrI). La direction du projet doit vérifier elle-même ou avec l'aide du préposé à la protection des informations de son office, de son département ou de la ChF si des informations classifiées sont traitées ou seront créées dans le cadre du projet :

- C'est facile à vérifier, car la mention de classification se trouve toujours en haut à droite, au moins sur la première page d'un document (WordDok, Excel, PowerPoint). Si des supports d'informations sont regroupés physiquement dans un recueil, il faut contrôler si celui-ci doit être classifié ou recevoir un échelon de classification supérieur (cf. art. 4, al. 2, OPrI). Si la direction du projet soupçonne que les informations à traiter sont attribuées à un échelon de classification trop élevé (ce qui est souvent le cas dans l'administration fédérale), il est possible de soumettre la classification à une nouvelle évaluation. La modification de la classification d'un document, d'une série de documents ou d'un type de document ne peut toutefois être effectuée que par la personne ou l'office dans l'intérêt duquel le secret est gardé (détenteur du secret) et ne peut pas être effectuée par la direction du projet elle-même (cf. art. 4, al. 1, OPrI). La modification de la classification peut avoir une influence considérable sur les mesures techniques de protection des systèmes, des logiciels ou du matériel, sur les ressources nécessaires ainsi que sur les coûts du projet et donc sur le succès d'un projet, en raison des prescriptions de traitement différentes prévues à l'art. 18 OPrI pour les informations classifiées INTERNE, CONFIDENTIEL ou SECRET, car les informations classifiées CONFIDENTIEL nécessitent des mesures de protection plus strictes (notamment un cryptage suffisamment fort). Cela implique des coûts plus élevés et, le cas échéant, nécessite de ressources supplémentaires pour un projet.
- La direction du projet devra donc veiller à ce que les informations (cf. art. 3, let. a, OPrI) ou les supports d'information (cf. art. 3, let. b, OPrI) créés dans le cadre du projet soient classifiés conformément aux dispositions des art. 4 à 9 OPrI et à sensibiliser les collaborateurs du projet sur ce point. Le regroupement d'informations ou de supports d'information dans le nuage peut, de manière imprévue, constituer un recueil, ce qui peut nécessiter une adaptation de la classification ou la création d'un nouvel élément à classifier (cf. art. 4, al. 2, OPrI).

Si des informations dignes de protection classifiées INTERNE ou CONFIDENTIEL conformément à l'OPrI sont traitées dans un nuage public ou si une application nuagique doit être mise en service dans le cadre d'un projet, la direction du projet doit observer ou vérifier les points suivants :

[122] Voir la compilation des prescriptions relatives aux mesures de protection des informations pour les collaborateurs de l'administration fédérale, sous la forme d'une directive de l'UPIC du 1er avril 2020 fondée sur l'OPrI (feuille d'information orange.
[123] https://www.vtg.admin.ch/content/vtg-internet/fr/service/info_trp/sicherheit/_jcr_content/contentPar/tabs_copy/items/downloads/tabPar/downloadlist/downloadItems/190_1472734389467.download/52_059_f.pdf

- **Question fondamentale :** quel type d'informations classifiées sera traité ou créé dans le cadre du projet ? En conséquence, l'OPrI, y compris les prescriptions de traitement et le catalogue de classification, s'applique ou non.
- **Question subsidiaire :** quelles sont les autres dispositions et directives de la Confédération, du département ou de l'unité administrative qui s'appliquent aux informations classifiées, en plus de la protection informatique de base[124] et du droit en vigueur (par ex. les instructions ou directives de la Confédération ou des départements, comme la stratégie d'informatique en nuage de l'administration fédérale, la stratégie d'informatique en nuage du département) ?

Si l'OPrI est applicable, la direction du projet doit notamment s'assurer que la procédure de sécurité visée aux art. 14*d* ss. en relation avec l'art. 3, let. h, OPCy (objet informatique à protéger; service nuagique en tant qu'objet informatique à protéger) est intégrée dans le projet et exécutée correctement. La conformité au droit est toujours donnée lorsque les risques résiduels identifiés sont pris en charge par l'organe compétent. S'il est établi que le projet correspond à l'état actuel de la science et de la technique, une pondération des risques et de l'utilité peut être entreprise. Si celle-ci est clairement en faveur de l'utilité, les risques résiduels peuvent être assumés.

Si aucune information classifiée n'est traitée ou créée dans le cadre du projet nuagique (voir ci-dessus), l'OPrI ne s'applique pas. Cela devrait être souvent le cas, car selon des estimations internes, environ 90 % des informations de l'administration fédérale ne sont pas classifiées. Par contre, l'OPrI s'applique si seule une petite partie des informations concernées par un projet concret est classifiée.

4.2 Future loi sur la sécurité de l'information (LSI)

4.2.1 Principales nouveautés de la LSI

La LSI vise à garantir la sécurité du traitement des informations, y compris des informations non classifiées, relevant de la compétence de la Confédération, sous l'angle de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité, ainsi que la sécurité des moyens informatiques de la Confédération. Selon l'art. 5, let. a, LSI, on entend par *moyen informatique* un moyen relevant des techniques de l'information et de la communication, notamment les applications, les systèmes d'information et les fichiers, ainsi que les installations, les produits et les services servant au traitement électronique des informations.

Pour garantir la sécurité de l'information lors de l'utilisation de moyens informatiques, en particulier lors de l'acquisition de prestations informatiques auprès de fournisseurs externes, les dispositions relatives à la sécurité des moyens informatiques visées aux art. 16 à 19 LSI sont désormais déterminantes (les art. 16 à 19 LSI remplacent les art. 14*b* à 14*e* OPCy).

Le champ d'application institutionnel de la LSI est plus étendu que celui de l'OPrI. La loi s'applique à toutes les autorités fédérales (Assemblée fédérale, Conseil fédéral, tribunaux de la Confédération, Ministère public de la Confédération et son autorité de surveillance et Banque nationale suisse : autorités concernées visées à l'art. 2, al. 1, LSI) et aux organisations qui leur sont subordonnées (départements, Chancellerie fédérale, unités administratives de l'administration fédérale centrale et de l'administration fédérale décentralisée : organisations concernées visées à l'art. 2, al. 2, LSI). Les organisations de droit public ou privé chargées de tâches fédérales sont assimilées aux organisations concernées et sont soumises à la LSI. Le Conseil fédéral peut toutefois, par voie d'ordonnance, exclure du champ d'application de la LSI ou de certaines parties de la LSI les organisations de l'administration fédérale décentralisée et des organisations de droit public ou privé qui sont chargées de tâches administratives (art. 2, al. 3 et 4, LSI). Les cantons doivent aussi se conformer à certaines dispositions de la LSI s'ils ne garantissent pas une sécurité au moins équivalente de l'information lorsqu'ils accèdent aux moyens informatiques de la Confédération. Les tiers, qui n'e sont pas soumis à la LSI, doivent être tenus de respecter les dispositions celle-ci par des accords contractuels (cf. art. 9 LSI) ou, si les conditions sont réunies, être soumis à la procédure de sécurité relative aux entreprises (art. 49 ss LSI).

Le seuil des échelons de classification (INTERNE, CONFIDENTIEL, SECRET) est relevé : à l'avenir, ce qui est aujourd'hui classifié CONFIDENTIEL relèvera de l'échelon INTERNE. Le nombre d'informations classifiées en sera radicalement réduit, ainsi que celui des contrôles de sécurité des personnes

[124] La nouvelle protection informatique de base dans l'administration fédérale est entrée en vigueur le 1er mars 2022.

(CSP). Les critères de classification seront à l'avenir définis en détail dans l'ordonnance sur la sécurité de l'information (cf. AP-OSI, art. 17 ss).

La notion d'activité sensible, déterminante pour l'exécution des CSP et des procédures de sécurité relatives aux entreprises (anciennement procédures visant à sauvegarder le secret) est inscrite dans la loi (art. 5, let. b, LSI). Elle comprend le traitement d'informations classifiées CONFIDENTIEL et SECRET (art. 13, al. 2 et 3, LSI), l'administration, l'exploitation, la maintenance et le contrôle de moyens informatiques de protection élevée et de protection très élevée (art. 17 LSI) et l'accès aux zones de protection 2 et 3 d'une installation au sens de la législation sur les ouvrages militaires.

La sécurité de l'information s'alignera à l'avenir sur les normes internationales, un système de gestion de la sécurité de l'information (SGSI), le niveau d'ambition de la sécurité et les mesures correspondantes étant définis. Le SGSI augmente la protection minimale requise des informations et des moyens informatiques par rapport aux exigences actuelles de l'OPCy et de l'OPrI.

4.2.2 Mise en oeuvre de la LSI : travaux en cours

La LSI a été adoptée par le Parlement le 20 décembre 2020. Le délai référendaire a expiré le 12 avril 2021 sans avoir été utilisé. L'élaboration des dispositions d'exécution de la LSI est en cours, sous la direction du SG-DDPS dans le but de faire entrer en vigueur la loi et ses ordonnances le 1er juillet 2023[125]. La LSI remplacera l'OPCy et l'OPrI dès son entrée en vigueur.

Différentes dispositions d'application de la LSI sont en cours d'élaboration[126]. L'OPrI sera abrogée à l'entrée en vigueur de la LSI. L'OPCy sera abrogée et ses dispositions (en partie adaptées) seront intégrées dans la future ordonnance sur la sécurité de l'information (OSI). L'ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (RS *172.010.59*) sera partiellement révisée.

L'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP, RS *120.4*) sera abrogée et une partie des dispositions de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS *120*) sera intégrée dans la future ordonnance sur les contrôles de sécurité relatifs aux personnes.

L'ordonnance concernant la sauvegarde du secret (RS *510.413*) sera abrogée et remplacée par la future ordonnance sur la procédure de sécurité relative aux entreprises (OPSE). Le champ d'application de la PSE, strictement militaire aujourd'hui, sera étendu au domaine civil.. Les fournisseurs de services de nuages privés devront donc se soumettre à une PSE s'ils exercent pour la Confédération une activité sensible au sens de l'art. 5, let. b, LSI. Dans le présent contexte, par activité sensible on entend le traitement d'informations classifiées CONFIDENTIEL ou SECRET et l'administration, l'exploitation, la maintenance et le contrôle de moyens informatiques relevant des catégories de sécurité «protection élevée» ou «protection très élevée». L'OPSE remplacera le GRAES. Enfin, la révision totale de la LSI introduira une obligation de signaler les cyberévénements contre des infrastructures critiques[127].

4.2.3 Conséquences de l'entrée en vigueur de la LSI pour les projets nuagiques

La LSI règle deux points déterminants pour l'utilisation d'une solution nuagique dans son champ d'application concernant les informations à traiter dans le nuage (classifiées ou non classifiées) et concernant le résultat de la PSE, si un moyen informatique relève de la catégorie de sécurité «protection de base», «protection élevée» ou «protection très élevée» conformément à l'art. 17 LSI.

Il conviendra notamment d'examiner les points suivants :

- *Classification* : les informations classifiées conformément à l'OPrI devront être adaptées aux nouvelles règles de classification à l'entrée en vigueur de la LSI (art. 11 à 15 LSI en relation avec la future OSI) dès leur premier traitement (par ex. enregistrement, modification, effacement, etc.) (cf. art. 90, al. 1, LSI).

[125] Pour toute question concernant l'état d'avancement du projet « Mise en œuvre de la LSI », veuillez vous adresser à Christophe Perron (chef de projet) ou à Melanie Koller (chef de projet adjointe). Un site Intranet concernant la LSI est en préparation.
[126] Calendrier de la mise en œuvre de la LSI à la mi-janvier 2022 : 1re consultation des offices vers la fin février 2022 ; consultation du 24 août au 24 novembre, entrée en vigueur au 2e semestre 2023.
[127] Pour toutes questions relatives à l'obligation de signalement de cyberévénements contre des infrastructures critiques, veuillez vous adresser à Manuel Suter (SG-DFF).

- Les *moyens informatiques* (art. 5, let. a, LSI) doivent être classés dans un délai de deux ans à compter de l'entrée en vigueur de la LSI (art. 16 à 19 LSI en relation avec l'OSI). Les mesures techniques visant à assurer la sécurité de l'information doivent être mises en place dans un délai de six ans à compter de l'entrée en vigueur de la LSI (art. 90, al. 2, LSI). Une application nuagique est également considérée comme un moyen informatique, ce qui signifie que la LSI et toutes les dispositions d'exécution correspondantes s'appliquent aux projets nuagiques.
- *Contrôles de sécurité relatifs aux personnes (CSP)* : les déclarations relatives à la sécurité des personnes et les déclarations relatives à la sécurité des entreprises rendues selon l'ancien droit sont valables cinq ans à compter de leur établissement (art. 90, al. 3, LSI), la direction de projet n'a donc rien à faire en ce qui concerne les CSP existants. Il en va autrement pour les nouveaux collaborateurs du projet : dans ce cas, la direction du projet a le droit, en collaboration avec le mandant, d'exiger que les CSP des nouveaux collaborateurs soient conformes aux nouvelles dispositions de la LSI.
- *Procédure de sécurité relative aux entreprises (PSE)* : les déclarations relatives à la sécurité des entreprises rendues selon l'ancien droit sont valables cinq ans à compter de leur établissement (art. 90, al. 3, LSI), la direction du projet doit donc s'assurer, pour les mandats sensibles, que le soumissionnaire dispose d'une déclaration valable et fera si nécessaire appel au service spécialisé PSE (cf. procédure visée par l'OPSE). Si aucune déclaration n'a encore été délivrée, il faudra en faire établir une cf. procédure visée par l'OPSE). Désormais, les mandants de l'administration fédérale civile sont également tenus de déclencher une PSE (et non plus seulement le DDPS conformément à l'ordonnance concernant la sauvegarde du secret).

5 Autres bases légales pertinentes

5.1 Ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

L'ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM, RS *172.010.59*) règle les compétences, le traitement et la publication de données personnelles ainsi que les exigences concernant la sécurité de l'information pour les systèmes de gestion des données d'identification (systèmes IAM), les services d'annuaires et la base centralisée des identités de la Confédération (art. 1 OIAM). La section 5 (art. 15 ss) OIAM règle la communication des données. L'art. 17 OIAM règle la communication de données personnelles à un exploitant externe. Selon l'art. 17, al. 1, OIAM, les données personnelles issues des systèmes IAM peuvent en principe être communiquées à l'exploitant externe. L'art. 17, al. 2 à 4, OIAM énumère les conditions et les obligations qui doivent être respectées pour que la communication de données personnelles à des exploitants externes soit licite[128]. L'art. 18 OIAM règle les exigences concernant la sécurité de l'information. L'OIAM règle donc explicitement l'externalisation dans le nuage et l'autorise pour les systèmes IAM aux conditions énoncées aux art. 17 ss.

L'OIAM fait actuellement l'objet d'une révision partielle et la modification devrait entrer en vigueur le 1er juillet 2023, en même temps que la LSI. Aucune adaptation des articles susmentionnés n'est prévue (état : février 2022).

5.2 Prescriptions concernant le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération

Les art. 57*i* ss de la loi sur l'organisation du gouvernement et de l'administration (LOGA, RS *172.010*) règlent le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique (données secondaires) à titre subsidiaire, lorsqu'aucune autre loi fédérale ne règle la question. L'art. 57*j*, al. 1, LOGA établit le principe selon lequel les unités administratives ne sont pas autorisées à enregistrer et analyser les données personnelles liées à l'utilisation de leur infrastructure électronique.

Les art. 57*l* à 57*o* LOGA règlent les cas dans lesquels des données personnelles peuvent être enregistrées, en particulier : copies de sauvegarde, entretien, contrôle du respect des règlements d'utilisation, traçabilité de l'accès. Les art. 57*m* et 57*n* LOGA règlent les analyses ne se rapportant pas aux

[128] Notamment l'information préalable des personnes concernées (art. 17, al. 4, OIAM).

personnes et les analyses non nominales se rapportant aux personnes. L'art. 57*o* LOGA règle les analyses nominales se rapportant aux personnes. Celles-ci sont notamment licites pour analyser les perturbations de l'infrastructure électronique, y remédier ou parer aux menaces concrètes qu'elle subit (let. b). Les analyses visant à élucider un soupçon d'utilisation abusive ne sont autorisées que si elles sont effectuées par les organes de la Confédération et après information écrite de la personne concernée.

Enfin, les unités administratives doivent prendre les mesures techniques et organisationnelles nécessaires pour prévenir les abus. Pour les projets d'informatique en nuage, cela signifie notamment qu'il faut veiller à ce que les données secondaires (par ex. journaux d'accès) soient protégées de manière adéquate et que l'accès à ces données soit clairement réglé et régulièrement contrôlé.

L'art. 1 de l'ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération (RS *172.010.442*) établit une distinction entre les données administrées et les données non administrées. Les données administrées sont des données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure électronique de la Confédération et qui sont régulièrement utilisées, analysées ou effacées volontairement. Il s'agit par exemple des journaux d'accès aux systèmes d'information ou des données concernant l'utilisation des systèmes de fermeture. Les données non administrées sont des données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure électronique de la Confédération, mais qui ne sont pas régulièrement utilisées, analysées ou effacées volontairement. Il s'agit par exemple des données enregistrées par une imprimante sur des ordres d'impression traités.

Seuls ont droit d'accéder aux données administrées l'exploitant du système et les services désignés par les directives de l'organe fédéral concernant la protection des données. L'art. 1, let. c, de l'ordonnance définit l'exploitant du système le service chargé de la gestion technique de l'infrastructure électronique de la Confédération. Les fournisseurs de services nuagiques sont mandatés par la Confédération, ils sont des exploitants du système au sens de l'ordonnance. Ils peuvent donc accéder aux données secondaires pour les finalités prévues par la loi. Seul l'organe fédéral qui utilise les appareils sur lesquels les données non administrées sont enregistrées a le droit d'accéder à ces données.

5.3 Ordonnance sur la gestion électronique des affaires dans l'administration fédérale (ordonnance GEVER)

Le champ d'application de l'ordonnance GEVER est très étendu : l'ordonnance s'applique à l'administration fédérale centrale et dans certains cas aux unités décentralisées ; elle s'applique aux systèmes de gestion des affaires standardisés ou non standardisés (art. 3)

Dans le domaine des systèmes standardisés, l'utilisation du nuage devrait être prévue et réglée dans les spécifications standard. Dans le domaine des systèmes non standardisés, des prescriptions particulières de l'ordonnance GEVER doivent être respectées en cas d'externalisation dans le nuage. Il s'agit notamment des prescriptions concernant le traitement d'informations classifiées (art. 11) et la journalisation (art. 13).

5.4 Directives applicables à toute l'administration fédérale

Différentes directives, valables pour l'ensemble de l'administration fédérale, peuvent être pertinentes pour l'informatique en nuage. C'est par exemple le cas des directives d'application du secteur TNI ChF, fondées sur l'art. 17, al. 1, OTNI. Parmi celles-ci, les directives E027 – Directive d'application Communication vocale chiffrée (CVC)[129] et E026 – Directive d'application sur le système de poste de travail[130] présentent un intérêt particulier. Les directives d'application concrétisent le droit supérieur : elles ne crées ni nouveaux droits ni nouvelles obligations pour les unités administratives.

En outre, la protection informatique de base dans l'administration fédérale[131], fondée sur l'art. 1, al. 1, let. e, OPCy est contraignante pour toutes les unités administratives (cf. partie 2).

[129] E027 - Directive d'application pour la communication vocale chiffrée (CVC)
[130] E026 - Directive d'application sur le système de poste de travail
[131] https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/vorgaben/sicherheit/si001/Si001-IT-Grundschutz-V5-0-f.pdf.download.pdf/Si001-IT-Grundschutz-V5-0-f.pdf

Annexe A Bibliographie et documents

BAERISWYL BRUNO	Wenn die Rechtsauslegung «nebulös» wird, in: digma 2019
BISCHOF SARAH	Partie 2: Die Bekanntgabe von Gesundheitsdaten / Kapitel 3: Datenschutzkonforme Bearbeitung von Gesundheitsdaten / V. Die datenschutzrechtlichen Grundsätze bei der Datenbekanntgabe / 1. - 6.; in: Datenschutz und Berufsgeheimnis im ambulanten Leistungsbereich (2020)
BLÖCHLINGER KARIN	Amtsgeheimnis und Öffentlichkeitsprinzip im Spannungsverhältnis, in: iusNet 2021
BRAUNECK JENS	Europa-Cloud: Zwingt der US CLOUD Act EU-Unternehmen zur EU-rechtswidrigen Datenherausgabe? In: Europäisches Wirtschafts- und Steuerrecht, 2019
Office fédéral de la justice	Bericht zum US CLOUD Act (loi Cloud), 2021
DICKINSON STEVE	China's new cybersecurity law: no place to hide, 11. Oktober 2020; https://harrisbricken.com/chinalawblog/china-cybersecurity-no-place-to-hide/ (24.3.2022)
HILLMANN JONATHAN E.	Digital Silk Road (2021)
KONFERENZ DER SCHWEIZERISCHEN DATENSCHUTZBEAUFTRAGTEN PRIVATIM	Merkblatt Cloud-spezifische Risiken und Massnahmen (V3 / 03.02.2022 (zit. Merkblatt privatim)
LAUX CHRISTIAN / HOFFMANN ALEXANDER	Rechtmässigkeit von Public Cloud Services, «Cloud-Gutachten» (unter Berücksichtigung des CLOUD Act), Rechtsgutachten an Organisation und Informatik der Stadt Zürich, 16. September 2021 (Link: Cloud Gutachten LLAG für OIZ (Sep 2021) mit Zusätzen (Nov 2021) (lauxlawyers.ch))
MICHLIG MATTHIAS; WYLER EVA	Art. 320 Verletzung des Amtsgeheimnisses, in: StGB annotierter Kommentar (2020)
MILLARD CHRISTOPHER	Cloud Computing Law, 2nd ed., Oxford University Press (2021)
ROSENTHAL DAVID	Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act; in: Jusletter du 10 août 2020
ROSENTHAL DAVID	Schweizer Banken in die Cloud; Vischer 9. September 2021 https://www.vischer.com/know-how/blog/schweizer-banken-in-die-cloud-so-geht-es-und-so-nicht-39214/
ROSENTHAL DAVID	Frequently Asked Questions (FAQ) on the Risk of Foreign Lawful Access and the Statistical "Rosenthal" Method for Assessing it, Version 1. August 2022, https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf (9.8.2022)
ROTH DAVID	Cloud-basierte Dienstleistungen im Licht der DSGVO in: Aktuelle Juristische Praxis, 2020
RUDIN BEAT	Bearbeiten im Auftrag in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), (2014)
SCHWARZENEGGER CHRISTIAN; THOUVENIN FLORENT; STILLER BURKHARD; GEORGE DAMIAN	Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, in: Anwaltsrevue 1/2019

STEINER THOMAS	Digitalisierter Arztbesuch und Cloud-Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, in: sic! 2020
THALNER CAROLINE	Das moderne Amtsgeheimnis im Spannungsfeld des Öffentlichkeitsprinzips, Masterarbeit UZH, 2019
VASELLA DAVID	Privatim – Merkblatt «Cloud-spezifische Risiken und Massnahmen» für öffentliche Organe: neue Fassung und kritische Anmerkungen; https://datenrecht.ch/privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-neue-fassung-und-kritische-anmerkungen/ (22.3.2022)
WIDMER URSULA	Gutachten Klärung und Analyse der rechtlichen Grundlagen für die Integration von «Platform-as-a-Service» und «Software-as-a-Service» in der öffentlichen Verwaltung für die Schweizerische Informatikkonferenz (SIK), 2018
WOHLERS WOLFGANG	Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), in: digma – Schriften zum Datenrecht Band/Nr. 9

Annexe B Glossaire

Gestion des clefs	Le niveau de cryptage doit tenir compte de la période spécifique pendant laquelle la confidentialité des données à caractère personnel cryptées doit être assurée. L'algorithme de cryptage doit être mis en œuvre sans erreur par un logiciel correctement maintenu, dont la conformité avec la spécification de l'algorithme choisi a été confirmée (par ex. par une certification). Les clefs doivent être gérées de manière fiable (générées, appliquées, stockées, le cas échéant, associées à l'identité du destinataire prévu et révoquées). **Bring Your Own Key (BYOK) ou Bring Your Own Encription (BYOE) :** l'unité administrative fournit les clefs de chiffrement, mais les confie au fournisseur de services nuagiques pour qu'il les gère et les utilise. Tant pour BYOK que pour BYOE, le processus de cryptage proprement dit a lieu dans le nuage, c'est-à-dire dans des systèmes gérés par le fournisseur de services. BYOE se distingue de BYOK, où on a le contrôle des clefs, par la possibilité supplémentaire de gérer soi-même également les algorithmes cryptographiques utilisés et, le cas échéant, les fonctionnalités. Du point de vue de la sécurité, les possibilités de contrôle supplémentaires offertes par BYOE ne jouent toutefois qu'un rôle négligeable. **Hold Your Own Key (HYOK) :** l'unité administrative reste toujours seule en possession des clefs. Dans l'idéal, ces données sont conservées sur un *Hardware Security Module* (HSM) qui peut lui-même être exploité virtuellement. Dans ce cas, on parle également de **Keep Your Own Key (KYOK),** l'organisation exerce un contrôle exclusif sur le HSM virtualisé et dans le nuage[132]. En conséquence, la clef n'est pas externalisée dans le nuage. Ce modèle vise à « empêcher que les données soient transmises en clair dans le nuage. Si elle est correctement mise en œuvre, cette procédure est incontestablement efficace pour empêcher un accès non souhaité aux données, mais elle implique encore, à l'heure actuelle, des pertes de fonctionnalité parfois importantes.
Sur site	« Sur site » (dans ses propres locaux, sur place ou localement) désigne un modèle d'utilisation et de licence pour des programmes informatiques (logiciels) basés sur un serveur.
Fournisseur de services nuagiques	Représente une entité qui établit une relation commerciale avec un consommateur et qui lui fournit un service qui fonctionne dans un centre de calcul sous le contrôle du fournisseur.
Nuage Services nuagiques Solutions nuagiques	Le nuage n'est pas une notion claire en soi et il est interprété de différentes manières. En résumé, la scalabilité à la demande, la disponibilité élevée et le partage des ressources, l'accès sécurisé et les accords de service sur mesures sont les caractéristiques généralement recherchées. Bien que certains de ces avantages soient déjà une réalité, de nombreuses tâches, en particulier dans le domaine de la sécurité, sont en développement permanent.
Mesures d'atténuation	Mesures visant à minimiser les risques
Utilisateur d'informatique en nuage, utilisateur du nuage	Utilisateur de services nuagiques
Sous-traitant	Un sous-traitant est un entrepreneur indépendant qui reçoit des commandes d'une entreprise générale (également appelée entreprise principale). Les conditions doivent être convenues contractuellement avec l'entreprise mandante, dans un contrat d'entreprise ou de service. Les sous-traitants se rencontrent surtout dans les segments de l'artisanat et des services.

[132] cloud-computing-2021-11-08.pdf

Fournisseur de services	Entité qui fournit un service spécifique, en faisant éventuellement appel à des fournisseurs de services nuagiques (sous-traitants).