AJP/PJA 6/2019

L'utilisation de l'informatique en nuage par l'administration publique

Sylvain Métille*

Le recours à des services informatiques en ligne est courant. Il n'en demeure pas moins soumis à des règles strictes pour l'administration. Si les exigences en matière de protection des données peuvent généralement être respectées dans le cadre de la négociation du contrat de services, il en va différemment du secret de fonction qui empêche le traitement de données hors de Suisse. Après avoir exposé ces limites, l'article présente encore quelques particularités des contrats informatiques.

Die Nutzung von Online-IT-Diensten ist weitverbreitet. Jedoch unterliegt sie weiterhin strengen Regeln für die Verwaltung. Bei der Aushandlung des Dienstleistungsvertrages können die datenschutzrechtlichen Anforderungen grundsätzlich erfüllt werden. Anders ist dies beim Amtsgeheimnis, das die Verarbeitung von Daten im Ausland verhindert. Nach der Darstellung dieser Einschränkungen geht der Artikel auf einige Besonderheiten von IT-Verträgen ein.

Plan

I. Introduction

Le recours à des services informatiques fournis par des tiers est devenu courant, à titre privé comme à titre professionnel. Certains sont même préinstallés sur nos téléphones portables à l'achat, et parfois très confortables à utiliser. Pourtant la confidentialité des données n'y est pas toujours garantie.

La situation est plus préoccupante lorsqu'il s'agit non seulement de ses propres données, mais également de données de tiers que l'on est responsable de traiter conformément à la loi et aux attentes de ces personnes. Pour l'administration publique[1], des règles particulières limitent encore plus le recours à des fournisseurs de services informatiques tiers, en particulier lorsque ces données sont protégées par le secret de fonction. Après s'être penché sur ce qu'il faut comprendre par un service fourni au travers de l'informatique en nuage (II.), nous allons examiner les règles à prendre en compte, notamment au regard du secret de fonction et de la protection des données (III.), ainsi que quelques éléments importants en lien avec les contrats informatiques en général (IV.).

II. Le Cloud

L'informatique en nuage (cloud computing ou cloud) recouvre des technologies et des modèles de services très différents accessibles en ligne, via un réseau informatique, depuis n'importe quel endroit, de sorte que leur emplacement physique peut être négligé d'un point de vue technique[2].

On distingue traditionnellement le cloud privé du cloud public. Le cloud privé appartient à celui qui l'utilise : c'est une infrastructure propre avec des ressources physiques dédiées (souvent un serveur géré à l'interne)[3]. Le cloud public quant à lui est une infrastructure proposée par un fournisseur d'hébergement tiers à de nom-

* Sylvain Métille, avocat et Docteur en droit, professeur associé à l'Université de Lausanne et responsable de la Maîtrise universitaire en Droit, Criminalité et Sécurité des technologies de l'information.
L'auteur remercie chaleureusement Me Nadja Nguyen Xuan et M. Livio di Tria pour leur aide dans la rédaction du présent article.

1 Qu'elle soit fédérale, cantonale ou communale.

2 Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller/Damian George, Utilisation des services de cloud par les avocats, Revue de l'avocat 2019, 25 ss, 33 ; Avis 05/2012 sur l'informatique en nuage adopté le 1er juillet 2012 par le Groupe de travail « Article 29 » sur la protection des données, 5.

3 Si des mesures de sécurité suffisantes sont prises, le recours au cloud privé ne représente guère de difficultés sous l'angle de la protection des données et du secret de fonction car il n'implique pas de traitement de données par un tiers.

breux clients qui en partagent l'utilisation[4]. Il existe de nombreuses variantes de cloud, certains garantissant une localisation déterminée des serveurs, voire une séparation logique voire physique des données d'un utilisateur.

Il existe ensuite différents modèles de cloud, notamment *l'Infrastructure-as-a-Service* (IaaS) et le *Software-as-a-Service* (SaaS). Dans le premier modèle (IaaS), les ressources de cloud telles que le stockage ou l'accès au réseau sont mises à disposition en tant que service. Avec ce modèle, l'administration (qui est le client d'un fournisseur tiers) continue de déterminer quelles solutions logicielles seront installées et elle doit prendre des mesures pour assurer la confidentialité et l'intégrité de solutions déployées. Dans le second modèle (SaaS), le fournisseur de cloud fournit via Internet une application logicielle conviviale pour l'administration. Avec ce modèle de service, ce ne sont pas uniquement les logiciels ou les données qui sont hébergées de manière décentralisée sur le cloud mais l'ensemble du traitement des données.

Lors de l'utilisation de services cloud public, les données ne sont plus traitées localement chez le client, mais chez le fournisseur de services. La transmission des données par Internet[5] comme l'enregistrement local chez le fournisseur[6] peuvent être chiffrés. Avec le modèle IaaS, les données peuvent être chiffrées par le fournisseur de services (tant l'administration que le fournisseur peuvent déchiffrer les données) ou par l'administration (elle seule a accès aux données déchiffrées). Avec le modèle SaaS, le fournisseur a le plus souvent besoin d'accéder aux données pour fournir le service[7], ce qui empêche un chiffrement par l'administration (à tout le moins sans que le fournisseur ne puisse déchiffrer les données).

Dans tous les cas la terminologie n'est pas toujours unanime et il ne suffit pas de s'arrêter au nom du service. Il convient au contraire de bien vérifier techniquement ce qui est proposé et comment. Le fournisseur de services cloud public est soit un sous-traitant, soit un tiers, conformément à la terminologie de la protection des données[8]. Il peut être en Suisse ou dans un pays étranger, ce qui est le cas pour la plupart des fournisseurs. Il peut finalement traiter les données là où il a son siège ou dans un autre pays.

III. Les limites à l'utilisation d'un service cloud public

A. En général

Le recours à l'utilisation d'un service cloud public ou d'un sous-traitant informatique est devenu fréquent ; le cas est d'ailleurs prévu par l'Ordonnance fédérale sur l'informatique et la télécommunication dans l'administration fédérale (OIAF ; RS 172.010.58). Avant de recourir à ce service, l'administration doit examiner si son choix est limité par certaines obligations légales découlant en particulier du Code pénal suisse (CP ; RS 311.0) et de la Loi fédérale sur la protection des données (LPD ; RS 235.1).

Aux termes de l'art. 7 al. 1 LPD, les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. L'al. 2 de cette disposition prévoit que le Conseil fédéral édicte des dispositions plus détaillées sur les exigences minimales en matière de sécurité des données.

La sécurité des données régit les mesures qui doivent être prises pour que des personnes non autorisées n'aient pas accès aux données en question[9]. Le principe de sécurité s'impose au secteur privé comme aux organes fédéraux[10] et les exigences de sécurité doivent également être observées par le mandataire à qui tout ou une partie du traitement est délégué[11].

Les composantes de la sécurité sont déclinées par l'art. 8 al. 1 de l'Ordonnance relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11) soit :

– la confidentialité (seules les personnes légitimées peuvent avoir accès à des données déterminées) ;
– la disponibilité ; et

---

4 Il ne doit pas être confondu avec le cloud étatique ou souverain, parfois aussi appelé cloud de service public, soit une infrastructure gérée par l'État dans le but de garantir aux utilisateurs une solution nationale.

5 Notamment par les protocoles HTTPS *(Hypertext Transmission Protocol Secure)* et TLS *(Transport Layer Security)*.

6 Avec une clé locale, p. ex., par la méthode de cryptage AES *(Advanced Encryption Standards)*.

7 Schwarzenegger/Thouvenin/Stiller/George (n. 2), 33–34.

8 Le sous-traitant ne traite les données que sur les instructions du responsable du traitement (appelé aussi maître du fichier) qui a préalablement décidé des données à traiter et du but du traitement. Un fournisseur d'hébergement sera traditionnellement un sous-traitant. Le tiers est un responsable du traitement indépendant (parfois un co-responsable du traitement), qui peut traiter les données dans son intérêt. Les instructions de l'administration seront générales et concerneront la mission à atteindre, mais non la manière dont les données doivent être traitées. Ce sera p. ex. le cas d'un fournisseur de solution de sécurité, qui décidera seul des données à traiter.

9 Philippe Meier, Protection des données : Fondements, principes généraux et droit privé, Berne 2011, N 780 ; Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht : Grundlagen und öffentliches Recht, Berne 2011, N 51.

10 Meier (n. 9), N 783 ; Wolfgang Straub, Vom Keller zur Cloud – digitales Arbeiten in der Anwaltskanzlei, Jusletter du 1.5.2017, N 16.

11 Meier (n. 9), N 784.

– l'intégrité (les données sont protégées contre des manipulations humaines ou par l'entremise de logiciels malveillants)[12].

À ce sujet, l'on peut encore mentionner l'art. 6 OIAF selon lequel l'utilisation des technologies de l'information et de la communication (TIC) présuppose que les bases légales suffisantes existent déjà ou seront créées (let. a) ; que la protection des données relatives aux personnes concernées est garantie (let. b) et que la sûreté intégrale de l'information est garantie (let. c).

Dans la mesure où la confidentialité est une composante de la sécurité des données, nous examinerons d'abord si le secret de fonction présente un obstacle à l'utilisation de services cloud et, si tel n'est pas le cas, nous examinerons quelles sont les conditions posées par la LPD pour que le traitement de certaines données puisse être délégué à un fournisseur.

B. Le secret de fonction (art. 320 CP)

1. Les éléments constitutifs de l'infraction

L'art. 320 al. 1 CP dispose que « celui qui aura révélé un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il avait eu connaissance à raison de sa charge ou de son emploi, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. La révélation demeure punissable alors même que la charge ou l'emploi a pris fin ».

La violation du secret de fonction est une infraction pénale, poursuivie d'office. Il s'agit d'un délit de mise en danger abstrait, ce qui n'implique pas qu'il y ait un résultat ou un dommage[13]. Il suffit qu'il soit possible d'obtenir les données couvertes par le secret. Il n'est pas nécessaire qu'elles aient été effectivement consultées.

Pour que l'infraction soit réalisée, plusieurs conditions doivent être remplies cumulativement :

a. Une personne soumise au secret de fonction

Premièrement, l'infraction ne peut être commise que par un membre d'une autorité ou un fonctionnaire[14]. La notion de fonctionnaire englobe toute personne ayant accompli sous la dépendance de l'État, une tâche publique, que ce soit à plein temps, à temps partiel ou simplement de manière temporaire, en tant qu'employé ou auxiliaire[15]. Ce n'est d'ailleurs pas la nature des relations de service ou du contrat de travail qui est déterminante pour savoir si une personne est soumise ou non au secret de fonction, mais la nature de l'activité exercée au service de la collectivité[16]. C'est la personne individuelle, soit le fonctionnaire jugé responsable, qui est condamné à titre individuel et non l'État.

b. Un fait secret appris dans l'exercice de la fonction

Deuxièmement, l'élément protégé n'est pas n'importe quelle information, mais seulement un fait secret. L'on rappellera à cet égard que toutes les informations ne sont pas secrètes. Le secret de fonction ne protège qu'un fait qui n'est connu ou accessible qu'à un cercle restreint de personnes, que son détenteur veut garder secret et qui y a un intérêt légitime[17]. On basculerait dans l'abus de droit si l'on admettait qu'il faut garder le secret au sujet de faits qu'il n'y a aucun intérêt à tenir confidentiels. Il faut donc un intérêt digne de protection à ce que le secret soit gardé[18].

Ce fait doit en outre avoir été appris dans le cadre de l'exercice de la fonction, ce qui signifie qu'il y a un lien direct entre la prise de connaissance et l'exercice de la fonction[19]. Il faut examiner les circonstances concrètes pour considérer que le fait a été appris à raison de sa fonction[20].

Le texte de l'art. 320 CP n'a pas changé depuis l'entrée en vigueur du CP en 1942, hormis la terminologie liée à la sanction[21]. Cela étant, la notion a évolué avec l'entrée en vigueur de la Loi fédérale sur le principe de la transparence dans l'administration (LTrans ; RS 152.3) le 1er juillet 2006 puisqu'elle a remplacé, au niveau fédéral, le principe de secret de l'activité des autorités étatiques par celui de la transparence[22]. Le principe de transparence a en effet

---

12 Meier (n. 9), N 786 ; BSK DSG/BGÖ-Bühler/Rampini, art. 7 DSG N 7, in : Urs Maurer-Lambrou/Gabor-Paul Blechta (édit.), Datenschutzrecht/Öffentlichkeitsgesetz, Basler Kommentar, Bâle 2014 (cit. BSK DSG/BGÖ-auteur).

13 Bernard Corboz, Les infractions en droit suisse, Volume II, 3e éd., Berne 2010, 745–746.

14 Corboz (n. 13), 738.

15 Michel Dupuis/Laurent Moreillon/Christophe Piguet/Séverine Berger/Miriam Mazou/Virginie Rodigari (édit.), Petit Commentaire du Code Pénal, 2e éd., Bâle 2017 (cit. PC CP), art. 320 N 11 ; Rolf H. Weber, Outsourcing von Informatik-Dienstleistungen in der Verwaltung, ZBl 1999, 97 ss, 118.

16 BSK StGB II-Oberholzer, art. 320 N 6, in : Marcel Alexander Niggli/Hans Wiprächtiger (édit.), Strafrecht II, Basler Kommentar, 3e éd., Bâle 2013 (cit. BSK StGB II-auteur).

17 CR CP II-Verniori, art. 320 N 14, et les références citées, in : Alain Macaluso/Laurent Moreillon/Nicolas Queloz (édit.), Code pénal II, Commentaire Romand, Bâle 2017 (cit. CR CP II-auteur).

18 Corboz (n. 13), 740.

19 CR CP II-Verniory (n. 17), art. 320 N 26.

20 PC CP (n. 15), art. 320 N 23.

21 CR CP II-Verniory (n. 17), art. 320 N 2.

22 PC CP (n. 15), art. 320 N 4. À noter que nombre de cantons ont également adoptés des lois similaires, appelées parfois aussi loi sur l'information.

été introduit dans le but de rendre le processus décisionnel de l'administration plus transparent dans le but de renforcer le caractère démocratique des institutions publiques de même que la confiance des citoyens dans les autorités, tout en améliorant le contrôle de l'administration[23].

Le principe du secret ne peut dès lors plus que s'appliquer aux faits qui sont exclus du champ d'application de la LTrans, soit des faits qui tombent sous le coup de l'une des exceptions de la LTrans ou sous le coup d'une disposition légale spéciale[24]. Viole donc le secret de fonction celui qui divulgue des documents officiels ne pouvant pas être rendus accessibles en vertu de la LTrans[25]. Pour décider s'il existe un intérêt digne de protection à ce que le secret soit gardé, il faut examiner le contenu des actes soumis au secret[26] pour vérifier si un intérêt privé ou public prépondérant s'opposerait à la divulgation.

Les intérêts publics prépondérants visent à assurer le bon fonctionnement des autorités et du processus de décision, ainsi que la sécurité et l'ordre publics, alors que les intérêts privés prépondérants assurent principalement la protection contre une atteinte notable à la sphère privée ou d'autres secrets.

L'intérêt privé existe lorsque la révélation des faits risque de porter préjudice à la personne en cause, notamment en cas de violation de sa sphère privée. Il y a un intérêt public au maintien du secret lorsqu'en cas de violation du secret, l'État, ses autorités ou leurs membres sont lésés dans leur patrimoine, leur honneur ou leur réputation, ou lorsqu'il en résulte pour eux d'autres difficultés[27], et lorsque l'État est atteint dans son bon fonctionnement. Un indice de la présence d'un intérêt légitime au maintien du secret est donné lorsqu'une loi prévoit un devoir de discrétion du fonctionnaire ou du membre d'une autorité[28].

Il faut encore que celui qui a intérêt au maintien du secret manifeste, expressément ou tacitement, la volonté de le faire respecter. Le plus souvent, cette volonté résulte des circonstances. Il n'est plus question de secret si la personne organise par exemple une conférence pour révéler les faits[29]. La révélation de faits notoires, largement connus ou largement accessibles n'est pas punissable, pas plus que la révélation de faits déjà communiqués ou susceptibles d'être communiqués sur requête en vertu de la législation applicable sur l'accès aux documents[30]. Des coordonnées personnelles qui se trouvent dans un annuaire téléphonique ou professionnel, des données d'entreprises qui résultent du registre du commerce, des données figurant dans les différents systèmes d'information du territoire ou que l'on peut trouver librement sur Internet ne sont pas secrètes, de même que des informations qui sont parues dans la presse (de tout genre) ou dans un ouvrage[31].

c. La révélation du secret

Troisièmement, la révélation est le fait de porter à la connaissance ou de rendre accessible le secret à un tiers qui ne fait pas partie du cercle des personnes autorisées[32]. La manière dont le secret est révélé est sans importance. Il peut s'agir d'une révélation par oral, par écrit, voire par actes concluants[33]. Il suffit, en définitive, que la personne soumise au secret ait rendu possible l'accès[34].

La communication à d'autres personnes soumises au secret de fonction peut également représenter une révélation : la question décisive est celle de savoir si des faits secrets quittent le cercle des personnes qui sont habilitées à le connaître. Une révélation n'interviendrait en revanche pas lorsque les personnes à qui l'on communique le fait secret appartiennent au cercle des personnes habilitées[35]. Ainsi, toute communication entre personnes soumises au secret n'est pas prohibée : deux juges d'un tribunal collégial ou deux gestionnaires de dossiers d'un même service d'aide sociale peuvent se prodiguer des conseils mutuels au sujet d'un dossier, et un fonctionnaire peut en référer à son supérieur hiérarchique direct. Il s'agit là d'un secret « partagé ».

En simplifiant, on pourrait ramener les conditions de partage de l'information à la « bonne marche du service », à condition d'entendre cette expression dans une acceptation large[36]. On peut retenir deux critères fonctionnels à cet égard, à savoir la compétence matérielle du demandeur de l'information ainsi que la nécessité de l'information dans sa mission légale. Dans l'examen du premier critère, il s'agit de se demander si l'information deman-

---

23 ATF 136 II 399.
24 BSK DSG/BGÖ-Blechta (n. 12), N 47 ad Erläuterung und Systematik des BGÖ et art. 1 BGÖ N 3.
25 Message du Conseil fédéral s'agissant de la LTrans, FF 2003 p. 1821 ; PC CP (n. 15), art. 320 N 4.
26 PC CP (n. 15), art. 320 N 20.
27 *Ibidem* et références citées.
28 *Ibidem* et références citées.
29 Corboz (n. 13), 740.
30 CR CP II-Verniory (n. 17), art. 320 N 19–21.
31 CR CP II-Verniory (n. 17), art. 320 N 19 et les jurisprudences citées.
32 PC CP (n. 15), art. 320 N 25.
33 Manon Jendly, La coexistence des secrets en exécution de peine privative de liberté, Neuchâtel 2005, 142.
34 Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB) / Externalisation du traitement des données personnelles et secret professionnel (art. 321 CPS), Zurich/Bâle/Genève 2016, 48.
35 Wohlers (n. 34), 49–50.
36 CR CP II-Verniory (n. 17), art. 320 N 31.

dée est bien en rapport avec la fonction du demandeur et son exercice, ce qui permet de limiter le cercle de personnes à qui l'information sera transmise. Dans l'examen du second critère, il s'agit de se demander si l'information demandée est nécessaire ou du moins utile à l'accomplissement de la mission du demandeur de l'information[37]. Ainsi, le fait de partager certaines informations avec un fournisseur de services cloud, en sa qualité d'auxiliaire, entrerait dans le cadre de la « bonne marche du service ».

Ainsi, il n'y aura pas de violation du secret de fonction lorsque le fait est communiqué à l'autorité supérieure ou qu'il est partagé au sein d'un groupe (secret collectif ou partagé), pour autant que tous les membres du groupe soient tenus à la même obligation de confidentialité et qu'ils aient connaissance des faits secrets dans et pour l'accomplissement de leurs tâches. Il n'y a pas non plus de révélation punissable lorsque la loi prévoit un devoir de collaborer avec une autre autorité administrative[38] ou une obligation de dénoncer[39].

d. L'intention

Enfin, l'auteur de la révélation n'est punissable que s'il a adopté volontairement un comportement qui a rendu le secret accessible ou s'il a à tout le moins accepté cette éventualité[40]. Ainsi, le dol éventuel au sens de l'art. 12 al. 2 CP est suffisant[41]. Il y aura violation de l'article 320 CP si l'auteur transmet le secret à un tiers, mais également s'il adopte un comportement dont il sait qu'il va permettre à un tiers de prendre connaissance du secret (dol éventuel)[42]. La violation du secret de fonction par négligence n'est pas punissable[43].

Lorsque des données sont partagées avec un fournisseur de services cloud, il faudra s'assurer que celui-ci respecte un certain nombre d'obligations afin d'éviter que les données couvertes par le secret ne soient rendues accessibles à des personnes non habilitées.

2. Les cas de révélations non punissables

a. La communication avec le consentement de l'autorité supérieure

L'art. 320 al. 2 CP prévoit que la révélation ne sera pas punissable si elle a été précédée du consentement écrit de l'autorité supérieure. La levée du secret est fréquente pour permettre aux collaborateurs de s'exprimer en tant que partie, témoin ou expert dans le cadre d'un interrogatoire ou d'une procédure judiciaire.

La levée du secret ne se fait toutefois pas à bien plaire. L'autorité supérieure doit procéder à une pesée stricte des intérêts en présence et il semble difficile de justifier la levée du secret lorsqu'elle ne sert qu'un intérêt technique ou économique de l'autorité (par exemple, un projet de sous-traitance qui pourrait être remplacé par une solution interne). Cela sera d'autant plus vrai que l'étendue des personnes et des domaines touchés par les données protégées est large.

Si l'autorité supérieure devait consentir à la révélation sans motifs suffisants, le fonctionnaire qui de bonne foi communique des informations couvertes par le secret ne devrait pas être inquiété[44]. L'autorité supérieure pourrait en revanche devoir assumer une responsabilité politique, voire juridique.

b. La communication à un auxiliaire

L'art. 320 CP ne mentionne pas expressément les auxiliaires, contrairement à l'art. 321 CP qui sanctionne la violation du secret professionnel. Pour que l'on ait affaire à un véritable auxiliaire au sens de cette disposition, il faut que ce dernier soit une personne effectivement apte à remplir la mission qui lui est confiée et qui accepte cette dernière[45]. Ainsi, seules les personnes qui participent effectivement à l'accomplissement des tâches liées à l'exécution des mandats doivent être tenues pour des auxiliaires[46]. Le professionnel peut révéler à ses auxiliaires un secret dont il a la garde dans la mesure où ces derniers lui sont nécessaires à l'accomplissement du mandat[47]. Ainsi, l'article 321 CP ne s'oppose pas à des services clouds dans la mesure où les auxiliaires sont également soumis au secret professionnel[48].

On doit appliquer la notion d'auxiliaire de l'art. 321 CP à l'art. 320 CP par analogie[49], en ce sens que les auxiliaires sont également soumis au secret de fonction, de

---

37 CR CP II-Verniory (n. 17), art. 320 N 32.
38 Actes autorisés par la loi (art. 14 al. 1 CP).
39 Article 22a de la Loi fédérale sur le personnel de la Confédération (LPers ; RS 172.220.1).
40 Corboz (n. 13), 746.
41 PC CP (n. 15), art. 320 N 33.
42 Corboz (n. 13), 746 ; CR CP II-Verniory (n. 17), art. 320 N 36 ; TF, 6B_599/2015, 25.2.2016, c. 2.3.
43 CR CP II-Verniory (n. 17), art. 320 N 36 et les références citées.
44 Il ne remplira pas la condition subjective de l'intention.
45 CR CP II-Chappuis (n. 17), art. 321 N 50.
46 CR CP II-Chappuis (n. 17), art. 321 N 76.
47 CR CP II-Chappuis (n. 17), art. 321 N 77.
48 Meier (n. 9), N 1227.
49 Weber (n. 15), 118.

sorte que la révélation du secret n'est pas punissable. Cela étant, il conviendra de poser des conditions strictes pour faire appel à un auxiliaire, lorsque les données qui lui sont communiquées sont soumises au secret de fonction.

Selon Wolfgang Wohlers, la communication d'un secret dans le cadre de l'externalisation ne sera pas pénalement sanctionnée lorsque le prestataire de services appartient au cercle des personnes habilitées à se voir confier un secret, ce qui implique que la communication du secret est indispensable pour l'accomplissement raisonnable de la prestation (a) et que le recours au prestataire de services est prévisible pour le titulaire du secret (b)[50]. Ce sera très rarement le cas en pratique. C'est une approche très restrictive de la notion d'auxiliaire, laquelle revient en définitive à n'intégrer que les fonctions qui sont indispensables à l'exercice des activités de l'État.

Il faut au contraire faire preuve d'un peu plus de souplesse et considérer que certains cas de délégations (et donc de reconnaissance de la qualité d'auxiliaire) doivent être admis lorsque cela est opportun, mais pas prévisible pour l'administré. En matière informatique notamment, il sera rarement prévisible pour l'administré que l'administration fasse appel aux services d'un sous-traitant. Cela sera toutefois souvent opportun si ce dernier est à même d'assurer un meilleur traitement des données ou une plus grande sécurité. C'est d'ailleurs le sens de l'article 26a OIAF. Admettre le principe du recours à un auxiliaire ne signifie pas encore que l'on puisse choisir n'importe quel auxiliaire, n'importe où.

Celui qui confie un secret à un auxiliaire doit s'assurer qu'il soit soumis au secret par la loi ou par un engagement exprès à garantir la confidentialité requise, notamment dans un contrat écrit[51]. Même si on lui accorde la qualité d'auxiliaire et une application automatique de l'art. 320 CP, il est vivement recommandé de le préciser dans le contrat de services.

Si un engagement à respecter le secret de fonction semble suffisant lorsque l'auxiliaire est en Suisse, il en va différent si celui-ci est soumis au droit étranger. Les autorités étrangères vont d'ailleurs appliquer prioritairement leur droit, ce qui pourrait conduire à ne pas respecter le secret de fonction au sens du droit suisse. L'auxiliaire pourrait ainsi être obligé, en vertu du droit étranger, à transmettre des informations protégées au sens du droit suisse. Il sera difficile de le sanctionner lorsqu'il agit à l'étranger et il pourra tout aussi difficilement se prévaloir d'un secret de fonction suisse pour éviter de devoir révéler les informations sur la base d'une requête valable en droit étranger[52].

Ainsi, il convient d'être particulièrement vigilant dans le choix de l'auxiliaire, non seulement en raison du fait que les données pourraient être communiquées à l'étranger mais également du fait qu'elles pourraient être détenues par une société étrangère. Cela est d'autant plus important depuis l'adoption par le Congrès américain du *Clarifying Lawful Overseas Use of Data Act* (« CLOUD Act ») en mars 2018. Ce texte permet désormais au gouvernement américain d'obtenir, sur la base d'un *warrant* ou d'un *subpoena,* les données qu'un fournisseur d'accès américain[53] détient, indépendamment de savoir si elles sont localisées sur le territoire américain ou à l'étranger[54].

Les personnes soumises au secret de fonction peuvent donc faire appel à un auxiliaire dans l'exécution de leurs tâches, moyennant toutefois le respect de certaines conditions, et notamment le traitement des données en Suisse, par une entité suisse.

c. Les données chiffrées

Les données anonymes peuvent être soumises au secret de fonction puisque ce secret protège également des données qui ne sont pas des données personnelles[55].

En pratique, la situation est d'autant plus compliquée car il s'agira souvent de données pseudonymes car une réidentification est possible[56]. Le groupe de travail « Article 29 » soulignait d'ailleurs que les techniques d'anonymisation peuvent apporter des garanties en matière de respect de la vie privée, mais que dans de nombreuses situations, un ensemble de données anonymes peut encore présenter un risque résiduel pour les personnes concernées[57]. On admet néanmoins que les données pseudonymes échappent à la LPD lorsque l'identification par un tiers ne paraît objectivement possible que moyennant des efforts qui apparaissent disproportionnés[58].

Selon les règles directrices du Préposé à la protection des données du canton de Zurich, le secret de fonction

---

50 Wohlers (n. 34), 58.

51 Weber (n. 15), 97.

52 Ursula Widmer, Gesundheitsdaten in der Cloud, D-A-CH Security 2011, 170 ; BSK DSG/BGÖ-Bühler/Rampini (n. 12), art. 10a DSG N 15 ; David Schwaninger/Stephanie S. Lattmann, Cloud Computing : Ausgewählte rechtliche Probleme in der Wolke, Jusletter du 11.3.2013, N 31.

53 Tel que défini par le droit américain.

54 Sebastian Cording/Lena Götzinger, Der CLOUD Act aus europäischer Sicht, Computer und Recht 2018, 636 ss, 636–637.

55 Straub (n. 10), N 6.

56 Meier (n. 9), N 446.

57 Avis 05/2014 sur les techniques d'anonymisation adopté le 10 avril 2014 par le Groupe de travail « Article 29 » sur la protection des données.

58 Meier (n. 9), N 447.

n'empêche en principe pas la délégation du traitement si les données sont chiffrées et si la gestion de la clé de chiffrement reste en mains du responsable du traitement[59]. Dans le même sens, l'aide-mémoire sur le cloud computing publié par l'association Privatim précise que lorsque les organes publics font de l'externalisation des données, ils doivent veiller à exclure ou réduire les risques spécifiques à un niveau acceptable par des mesures adéquates[60]. S'agissant de la protection des secrets et la gestion des clés, il est mentionné que les données doivent être chiffrées et, qu'en cas de données personnelles sensibles (y compris les données soumises à un secret professionnel ou à un secret de fonction particulier), des conditions supplémentaires doivent être posées quant à la gestion des clés et l'évaluation des risques[61].

Dans le cas où les données sont chiffrées et que le prestataire n'a ni la clé, ni la possibilité de déchiffrer les données, il ne s'agit pas de données personnelles et la LPD ne sera pas applicable[62]. Comme les données ne sont pas accessibles, il n'y aura pas non plus de violation du secret de fonction.

La difficulté est de savoir à partir de quand il faut retenir que la clé peut être retrouvée. Ce sera le cas si un tiers dispose de moyens susceptibles d'être raisonnablement mis en œuvre afin de l'obtenir, y compris à l'aide d'autres personnes ou d'une autorité compétente[63]. Ce ne sera en revanche pas le cas si la clé n'est pas compromise et que l'état actuel de la technique ne permet pas de la retrouver[64].

La clé pourrait être détenue exclusivement par le responsable du traitement, soit l'État, ou par un tiers de confiance qui n'aurait pas accès aux données. Des garanties contractuelles voire techniques doivent être mises en place pour s'assurer que le détenteur de la clé n'accède pas aux données ni ne communique la clé de déchiffrement[65]. La clé ne peut en revanche pas être administrée par le sous-traitant qui aurait alors accès aux données.

En pratique, un tel chiffrement est souvent réalisable lorsqu'il s'agit d'un simple hébergement de données auxquelles le sous-traitant n'a pas besoin d'avoir accès. On pourra alors chiffrer localement l'ensemble des données avant de les communiquer. Lorsqu'un service est fourni, et qu'il implique que les données soient accessibles au sous-traitant, le chiffrement n'est plus envisageable.

On peut donc conclure que si les données sont protégées par un chiffrement conforme à l'état actuel de la technique et que le sous-traitant (même à l'étranger) ne peut pas raisonnablement avoir accès à la clé, il n'y a pas de violation du secret de fonction[66]. Le même raisonnement s'appliquera en matière de protection des données.

d. Le consentement de la personne concernée

Le consentement préalable de l'individu concerné par le contenu du secret peut en principe constituer un fait justificatif à la violation d'un secret. Pour que le consentement donné par l'individu soit valable, il doit en outre être donné librement. Cela signifie que l'individu ne doit pas avoir subi de menace ou de pression déraisonnable de la part de l'auteur[67], et qu'il ne doit pas subir de préjudice en raison de son refus.

Le recours au consentement fonctionne bien pour le secret professionnel, mais rarement pour le secret de fonction. La doctrine admet certes de manière exceptionnelle qu'un consentement est suffisant pour permettre de lever le secret de fonction lorsque seul l'intérêt privé de celui qui consent est en jeu et à l'exclusion d'un quelconque intérêt public au maintien du secret[68].

Même si le consentement peut dans certains cas justifier l'externalisation et la révélation des secrets qu'elle implique, c'est une situation difficilement praticable dans la mesure où en réalité, il ne sera pas possible d'obtenir le consentement de toutes les personnes concernées. Ainsi, dans de telles situations, on doit soit séparer les données pour lesquelles on a obtenu le consentement de celles pour lesquelles on n'a pas obtenu de consentement, soit complètement renoncer à l'externalisation[69].

---

59 Datenschutzbeauftragter Kanton Zürich, Leitfaden Bearbeiten im Auftrag, version 1.3 octobre 2017, 5. Contrairement à ce que laissent penser ces règles directrices, ce n'est pas parce que le sous-traitant devient l'auxiliaire de l'administration (soumis au même devoir de conserver le secret) que le traitement à l'étranger est possible, mais bien parce que les données sont chiffrées et que la clé de chiffrement est seulement chez le responsable du traitement.

60 Privatim, Aide-mémoire Cloud Computing, V 1.0, 6 février 2019, 2.

61 Privatim (n. 60), 3. On peut d'ailleurs s'étonner que cet aide-mémoire qui traite de l'externalisation pour les organes publics ne mentionne que très brièvement le secret de fonction.

62 Pour le responsable du traitement qui a la clé ainsi que toute personne pouvant accéder ou déchiffrer les données, ce sera toujours des données personnelles.

63 CJUE, C582/14, 19.10.2016 par analogie, notamment § 48–49.

64 Voir également *Guidelines on Personal data breach notification under Regulation 2016/679* adoptées le 3 octobre 2017 par le Groupe de travail « Article 29 » sur la protection des données, 115–116.

65 Il semble également difficilement défendable qu'il soit à l'étranger si seules des garanties contractuelles l'empêchent de transmettre la clé.

66 Même un tiers devait, de manière illicite ou inattendue réussir à retrouver la clé, on ne peut pas retenir pénalement qu'il y a eu une intention de lui rendre les données accessibles.

67 Meier (n. 9), N 851.

68 PC CP (n. 15), art. 320 N 41 ; CR CP II-Verniory (n. 17), art. 320 N 52.

69 Wohlers (n. 34), 61.

Indépendamment des questions pratiques, le consentement de la personne concernée ne sera en général pas suffisant pour lever le secret de fonction puisqu'il y aura aussi un intérêt de l'État au maintien du secret.

e. D'autres faits justificatifs ?

On peut encore brièvement examiner d'autres faits justificatifs permettant de rendre la révélation non-punissable, notamment la question de l'intérêt prépondérant de la personne soumise au secret ou l'état de nécessité au sens de l'art. 17 CP. Tant le fait justificatif de l'état de nécessité au sens de l'art. 17 CP que celui de la prise en compte d'intérêts légitimes supposent que l'infraction intervienne pour protéger des intérêts prépondérants de l'auteur. En matière de services cloud, on ne peut pas en principe, prétendre que les intérêts économiques ou organisationnels de l'administration priment de façon claire l'intérêt au maintien du secret[70].

On ne peut pas non plus justifier l'absence de typicité pénale par l'argument du comportement usuel, la *Sozialadäquanz* (conformité aux normes sociales). Selon cette théorie, un comportement n'est pas punissable s'il se situe dans les limites de ce qui est absolument usuel, même si le comportement considéré réalise les conditions d'application d'une norme pénale. Cet argument est toujours délicat. En matière de services cloud, les conditions d'application de ce principe ne sont actuellement pas réalisées pour l'administration[71].

Cela étant, le recours à des prestataires informatiques en dehors de l'administration est devenu usuel et il serait difficile de s'en passer complètement. Le maître du secret a d'ailleurs un intérêt évident à ce que les meilleurs outils soient utilisés pour garantir la confidentialité, l'intégrité et la disponibilité des données. Ce sera au juge pénal d'interpréter dans quelle mesure la délégation de traitement est un risque admissible au sens de l'art. 320 CP ou s'il s'agit déjà d'une violation du secret de fonction.

L'art. 26a OIAF est un exemple concret, au niveau législatif, de définition par le Conseil fédéral d'un risque qu'il considère admissible. Si les conditions sont remplies, on devrait admettre que des mesures de précautions raisonnables ont été prises pour réduire au minimum l'atteinte au secret de fonction. Cet article légitime donc le recours de l'administration fédérale à des fournisseurs externes de prestations informatiques, mais ne permet pas pour autant le traitement à l'étranger[72].

C. La délégation du traitement des données personnelles

L'art. 10a LPD traite du traitement de données par un sous-traitant. L'al. 1 de cette disposition prévoit que le traitement de données personnelles peut être confié à un tiers pour autant qu'une convention ou la loi le prévoie et que les conditions suivantes soient remplies (let. a) seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués et (let. b) aucune obligation légale ou contractuelle de garder le secret ne l'interdit. L'al. 2 précise que le mandant doit en particulier s'assurer que le tiers garantit la sécurité des données.

Il faut donc d'abord un contrat entre l'administration et le fournisseur. Techniquement, on pourrait admettre qu'un contrat est valablement conclu par l'acceptation des conditions générales du fournisseur de services informatiques. Ces conditions sont souvent peu favorables à l'administration, voire représentent des risques importants comme l'application du droit étranger et d'un système d'arbitrage au lieu des tribunaux ordinaires, ou encore une limitation voire une exclusion de responsabilité. On préférera donc un contrat *ad hoc,* qui peut être négocié. La plupart des fournisseurs mettent d'ailleurs ce genre de contrats à disposition des entreprises/administrations et ils sont souvent beaucoup plus équilibrés, sans que des négociations importantes soient nécessaires.

Le contrat mentionnera l'identité de l'administration (ou de son service) et celle du fournisseur, le type et l'étendue du traitement, les catégories de données concernées, les technologies à mettre en œuvre, les accès, le développement et la maintenance des bases de données générées en sous-traitance, la sécurité, la localisation du matériel et le lieu d'où les services sont fournis, les instructions, contrôles et audits, le droit d'accès, l'éventuelle autorisation de sous-déléguer, ainsi que la durée de conservation et l'archivage des données. Il précisera

---

70 Wohlers (n. 34), 58–59. L'auteur y envisage toutefois un intérêt prépondérant de la personne soumise au secret dans des cas exceptionnels, comme p. ex. si, sans la révélation du secret, l'existence économique de la personne serait mise en danger.

71 Wohlers (n. 34), 57.

72 Le rapport explicatif relatif à cette disposition précise, s'agissant de l'accord écrit mentionné à la let. b que celui-ci ne correspond pas à l'autorisation de l'autorité supérieure au sens de l'article 320 al. 2 CP. En effet, l'accord écrit tel que prévu à l'article 26a let. b OIAF ne fait que prouver que le destinataire de la prestation a été informé par le prestataire de service interne que des prestataires de services externes interviendront dans le cadre d'une certaine prestation informatique. Si des secrets de fonction sont concernés, une autorisation de l'autorité supérieure au sens de l'article 320 al. 2 CP ainsi que les principes reconnus en jurisprudence devraient suffire à rendre la révélation non-punissable (Erläuterung zu Art. 26a E-BinfV du Département fédéral des finances).

encore que le sous-traitant n'a pas le droit d'utiliser les données dans son propre intérêt et qu'il est lié par les instructions du responsable du traitement[73]. Le contrat devra également garantir que des mesures techniques et organisationnelles suffisantes sont prises pour assurer la sécurité des données. Des mesures de sécurité plus élevées seront nécessaires en cas de traitement de données sensibles ou de profils de la personnalité[74].

La délégation n'est ensuite admise, aux termes de l'art. 10a al. 1 let. b LPD, que pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise. Lorsqu'une telle obligation existe, cela ne signifie pas que la délégation est automatiquement prohibée : il faut en revanche examiner sa licéité sous l'angle de cette disposition spéciale[75].

L'administration doit finalement s'assurer que le fournisseur garantisse la sécurité des données et respecte les autres principes. L'administration doit donc choisir le fournisseur avec soin, lui donner les instructions adéquates et exercer, dans la mesure du possible, la surveillance nécessaire pour que les instructions données soient respectées[76]. L'administration devrait, à intervalles réguliers, effectuer des audits de la sécurité auprès du fournisseur : elle devrait donc garder une possibilité d'accéder aux données dont le traitement a été délégué[77]. L'on rappellera que l'administration répond du préjudice causé si elle a confié le traitement à un fournisseur sans avoir pris les précautions nécessaires, dans son choix, ses instructions ou son contrôle, pour que celui-ci se conforme aux règles de la LPD[78].

Indépendamment des obligations légales précitées, l'administration doit encore vérifier l'opportunité et le risque de communiquer certaines données à un sous-traitant. Même s'il a légalement et contractuellement l'interdiction d'utiliser les informations auxquelles il a accès dans son propre intérêt, il y a des situations que l'administration préférera ne pas tenter. On peut par exemple penser à un sous-traitant qui traite pour l'administration les réponses à un appel d'offres auquel il participe également, ou qui héberge les liste de prix et factures d'un concurrent ou les postulations de candidats qui sont actuellement ses employés.

D. La communication transfrontière des données personnelles

Le recours à un sous-traitant informatique, en particulier s'agissant de l'hébergement ou de services fournis en ligne, implique souvent une communication de données à l'étranger.

Selon l'art. 6 al. 1 LPD, aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat. L'al. 2 de cette disposition prévoit les conditions auxquelles des données personnelles peuvent être communiquées à l'étranger en dépit de l'absence d'une législation assurant un niveau de protection adéquat.

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) publie une liste des pays considérés comme adéquats pour les données de personnes physiques[79]. Le transfert de données à une société américaine ayant adhéré au *Swiss-U.S. Privacy Shield* est assimilé à un transfert vers un pays adéquat[80]. Il est important de relever que le fait qu'un pays soit considéré comme adéquat n'a pas d'impact sur la violation éventuelle du secret de fonction.

Les garanties contractuelles peuvent prendre différentes formes. Le Conseil de l'Europe, l'Union européenne et le PFPDT proposent des contrat-types. En pratique, on recourt le plus souvent, en particulier pour en favoriser l'acceptation par le destinataire étranger, aux clauses contractuelles types de la Commission européenne que l'on aura pris soin d'amender pour qu'elles fassent référence au droit suisse et cas échéant cantonal. Comme il s'agit d'un cas de transfert du responsable du traitement

---

73 Meier (n. 9), N 1216 ; BSK DSG/BGÖ-Bühler/Rampini (n. 12), art. 10a DSG N 12.

74 Wolfgang Straub, Cloud Verträge – Regelungsbedarf und Vorgehensweise, PJA 2014, 905 ss, 915.

75 Meier (n. 9), N 1224 ; BSK DSG/BGÖ-Bühler/Rampini (n. 12), art. 10a DSG N 13.

76 Meier (n. 9), N 1218 ; BSK DSG/BGÖ-Bühler/Rampini (n. 12), art. 10a DSG N 11 et 15a ; Belser/Epiney/Waldmann (n. 9), 588–589, N 43.

77 Meier (n. 9), 432–433, N 1237 ; BSK DSG/BGÖ-Bühler/Rampini (n. 12), art. 10a DSG N 15a ; Belser/Epiney/Waldmann (n. 9), 594–595, N 54.

78 Meier (n. 9), N 1239.

79 Y figurent les pays suivants : Allemagne, Andorre, Argentine, Autriche, Belgique, Bulgarie, Canada, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Gibraltar, Grèce, Guernesey, Hongrie, Île de Man, Îles Féroé, Irlande, Islande, Israël, Italie, Jersey, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Monaco, Norvège, Nouvelle-Zélande, Pays-Bas, Pologne, Portugal, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Uruguay. Il n'y a pas de pays adéquats s'agissant des données relatives des personnes morales.

80 Le *Swiss-US Privacy Shield* (parfois appelé bouclier de protection des données personnelles) est un programme de certification auquel certaines entreprises peuvent adhérer et qui garantit un traitement similaire à celui qui aurait lieu dans un pays adéquat. Par analogie avec le *Safe Harbor :* Meier (n. 9), N 1333.

vers un sous-traitant, on utilisera le modèle contenu dans la Décision de la Commission européenne C(2010)593 du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (contrat-type). Ces garanties contractuelles sont généralement bien acceptées par les fournisseurs étrangers.

La validité de ce contrat-type, comme celle de toutes les autres garanties contractuelles, est actuellement remise en cause devant la Cour de justice de l'Union européenne (CJUE)[81]. En l'état, on doit cependant admettre que ce contrat est valable et qu'il peut être utilisé valablement par l'administration pour respecter ses obligations légales. En revanche, et même si le consentement de la personne concernée est également un motif justificatif autorisant le transfert, il est difficile à obtenir en pratique. Se posera également la question de la liberté de l'administré à consentir. Sauf cas particulier, il est préférable de renoncer à cette justification.

IV. Quelques particularités des contrats informatiques

A. La qualification juridique du contrat

Lorsque les conditions légales sont remplies, l'administration va pouvoir négocier[82] et conclure un contrat informatique[83]. Ces contrats doivent couvrir des prestations très techniques et prendre en compte des risques et des enjeux spécifiques. Il ne suffit pas de se limiter aux questions de protection des données et de secret de fonction, mais il faudra intégrer les aspects techniques tant dans la description des prestations fournies, que dans la qualification du contrat.

Les contrats informatiques, y compris ceux portants sur des prestations fournies à distance, ne sont pas définis en tant que tels par le Code des obligations (CO ; RS 220). Le régime juridique applicable doit être déterminé d'après les caractéristiques particulières de chaque cas. En effet, devant les différentes constellations de prestations prévues par des contrats informatiques, le Tribunal fédéral a adopté une approche pragmatique, au cas par cas et a ainsi refusé de procéder à la qualification *in abstracto* de ces contrats, considérant qu'une telle qualification devait se faire en tenant compte de la prestation litigieuse et des obligations des parties[84]. Comme on aura souvent à faire à des contrats innomés[85], le contenu du contrat sera d'autant plus important pour déterminer la volonté des parties[86].

Dans la pratique, la qualification nécessitera souvent d'interpréter le contrat en recherchant la réelle et commune intention des parties[87], en tenant compte du sens objectif des termes utilisés[88]. C'est ainsi la substance du contrat et les prestations qu'une partie s'est engagée à fournir en contrepartie d'un prix qui sera déterminante[89]. Lorsque l'interprétation littérale laisse subsister un doute sur l'intention des parties, il conviendra également de tenir compte des communications et pourparlers qui ont précédé la conclusion du contrat et, en particulier, des conditions que l'un des contractants a communiquées à l'autre au début de leur relation d'affaires[90].

L'enjeu de la qualification juridique a des effets concernant l'application des dispositions impératives prévues par la loi, auxquelles les parties ne peuvent pas valablement déroger. De même, si les aspects secondaires de la prestation sont insuffisamment décrits par le contrat, les parties, ainsi que le juge cas échéant, pourront se reporter aux règles supplétives.

---

81 La CJUE a invalidé la décision de la Commission européenne selon laquelle les États-Unis d'Amérique garantissaient un niveau de protection adéquat au travers de l'accord sphère de sécurité *(Safe Harbor)* conclu entre l'Union européenne et les États-Unis (arrêt CJUE C-362/14 du 6 octobre 2015) ce qui a conduit au remplacement du *Safe Harbor* par le *Privacy Shield,* y compris pour son homologue suisse. La *Irish High Court* a déposé le 9 mai 2018 une demande de décision préjudicielle présentée devant la CJUE visant notamment à établir la validité des clauses contractuelles types (Affaire C-311/18).

82 La capacité de négocier de l'administration dépend principalement de l'intérêt commercial que représente le projet pour le fournisseur.

83 Par contrat informatique, il ne faut pas entendre ici un contrat conclu de manière informatique, mais un contrat portant sur des prestations de nature informatique.

84 ATF 124 III 456 c. 4b/bb.

85 Les contrats innomés peuvent soit utiliser des éléments de contrats nommés dans une combinaison atypique, soit n'être assimilables à aucun modèle réglementé par la loi.

86 Même si les dispositions légales relatives aux principaux contrats légaux peuvent être appliquées par analogie pour compléter les dispositions du contrat lorsque celles-ci sont lacunaires ou comme moyen d'interprétation (Michel Jaccard/Vincent Robert, Les contrats informatiques, La pratique contractuelle : actualités et perspectives, Zurich 2009, 98).

87 Art. 18 CO.

88 ATF 131 III 606 c. 4.2.

89 Jaccard/Robert (n. 86), 106.

90 L'attitude des cocontractants avant la conclusion du contrat, pendant la phase de négociations, de même que les circonstances particulières dans lesquelles les parties ont déclaré leur volonté permettent parfois admettre une intention qui s'écarte du sens ordinaire des termes utilisés : ATF 131 III 606 c. 4.1 et 4.2 ; 130 III 417 c. 3.2.

La qualification d'un contrat informatique en un contrat de mandat ou d'entreprise a par exemple des conséquences très concrètes sur le régime de responsabilité, le mode de résiliation et la rémunération. Conformément aux règles de la garantie sur les défauts[91], l'entrepreneur répond de la prestation promise même sans faute, alors que le mandataire ne peut être tenu pour responsable que s'il a commis une faute. Concernant la résiliation du contrat, l'art. 404 CO, de nature impérative, autorise chacune des parties à résilier le contrat en tout temps, sans avoir à indemniser l'autre partie pour les conséquences de la résiliation, sous réserve de l'hypothèse de résiliation en temps inopportun[92]. Finalement concernant la rémunération, le mandataire a droit à une rémunération pour l'activité qu'il a exercée en vue du résultat recherché même s'il ne l'atteint pas, alors que l'entrepreneur est soumis à une obligation de résultat et ne peut être rémunéré que s'il obtient ce résultat[93].

B. Quelques exemples de contrats

Dans le domaine informatique, le contrat de licence joue un rôle important, en particulier lorsqu'il s'agit de services cloud ou de logiciels standards. Ceux-ci peuvent être protégés par divers droits de propriété intellectuelle (en particulier le droit d'auteur) et des obligations de confidentialité. En revanche, si le contrat porte sur la conception et la livraison de produits informatiques individualisés[94] répondant à des exigences spécifiques d'un client déterminé, les règles du contrat d'entreprise seront plus adaptées[95].

En effet, le contrat d'entreprise est un contrat par lequel l'entrepreneur s'oblige à exécuter un ouvrage, moyennant un prix que le maître de l'ouvrage s'engage à lui payer. Il consiste en un engagement ferme du prestataire d'atteindre un résultat déterminé. Le contrat d'entreprise se caractérise donc par une obligation de résultat, l'ouvrage supposant que le travail à effectuer puisse produire et garantir le résultat escompté[96]. Souvent, l'accord des parties sur une rémunération forfaitaire ou plafonnée pourra être interprété comme l'indice d'une volonté de soumettre le contrat aux règles du contrat d'entreprise[97]. Le contrat de développement de logiciel individualisé en fonction des besoins spécifiques de l'utilisateur[98] en constitue un exemple typique. Le contrat d'entreprise sera assez rare pour des services cloud, même s'il n'est pas exclu.

En revanche, lorsqu'il vise la fourniture de différents types de services, le contrat informatique peut être rapproché du contrat de mandat[99], qui constitue la forme la plus classique du contrat de services et dont les dispositions sont applicables par défaut pour les travaux qui ne sont pas soumis aux règles des autres contrats prévus par le CO[100]. En effet, le contrat de mandat est un contrat par lequel le mandataire s'oblige, dans les termes de la convention, à gérer l'affaire dont il s'est chargé ou à rendre les services qu'il a promis. Le mode de rémunération du prestataire et de facturation de ses prestations constitue un indice de la volonté des parties. Une facturation selon un tarif horaire et en tenant compte des coûts effectivement supportés par le prestataire (facturation dite en « régie ») sera un indice d'un contrat de mandat. En effet, le mandataire ne promet pas d'atteindre un résultat déterminé, mais il s'engage à fournir une activité en vue d'obtenir le résultat escompté par le mandataire[101].

L'accompagnement de l'administration dans le cadre d'une migration de données sur une nouvelle plate-forme informatique et les contrats prévoyant la planification, le conseil ou la gestion d'une certaine durée d'un projet informatique pour le compte d'un client ainsi que le contrat de maintenance constituent des exemples de contrats informatiques soumis aux règles du contrat de mandat. S'agissant du contrat de maintenance[102], il consiste à prévoir le maintien d'un système informatique dans un état de fonctionnement conforme aux exigences contractuelles convenues. Le prestataire peut s'engager soit à seulement réparer les erreurs de fonctionnement constatées (maintenance corrective), soit à améliorer le produit sous maintenance par des développements supplémentaires (maintenance évolutive). Si la maintenance corrective est souvent comprise dans un périmètre des prestations forfaitaires (par exemple liées à une licence), la maintenance évolu-

---

91 Art. 368 CO.

92 Art. 404 al. 2 CO. À noter toutefois que ce principe doit être relativisé dans la mesure où selon le Tribunal fédéral, l'art. 404 CO ne s'applique pas de manière systématique à l'ensemble d'un contrat informatique composé de prestations mixtes qui ne sont pas des prestations de pur service caractéristiques du contrat de mandat (ATF 109 II 462 c. 3.).

93 Art. 372 CO.

94 P. ex., des prestations d'intégration de données de l'administration.

95 ATF 124 III 456 c. 4b/bb.

96 Pierre Tercier/Laurent Bieri/Blaise Carron, Les contrats spéciaux, 5e éd., Zurich 2016, N 3513.

97 Jaccard/Robert (n. 86), 104.

98 TF, 4A_265/2008, 26.8.2008, c. 2.1.2.

99 Art. 394 ss CO.

100 Art. 394 al. 2 CO.

101 Art. 394 CO ; CR CO-Werro, art. 394 N 22, in : Luc Thévenoz/Franz Werro (édit.), Code des obligations I, Commentaire Romand, 2e éd., Bâle 2012.

102 Des prestations de maintenance peuvent aussi être prévues p. ex. comme des prestations annexes dans un contrat de fourniture de matériel ou de développement de logiciels.

tive est généralement vue comme une prestation supplémentaire facturée séparément.

Enfin un contrat en vertu duquel un prestataire informatique s'engage à héberger des données informatiques de son client contre rémunération se rapprochera *a priori* du contrat de bail à loyer, ou plus vraisemblablement du contrat de bail à ferme[103].

L'administration devra donc dans chaque cas de services cloud vérifier quelles prestations sont fournies et à quelles conditions, pour qualifier le contrat et connaître l'étendue de ses droits et obligations.

C. Le contenu du contrat

Un contrat lié à l'utilisation de l'informatique en nuage par l'administration doit couvrir les éléments essentiels nécessaires à tout contrat. On s'assurera en particulier d'avoir défini précisément les parties, le périmètre des prestations fournies et les modalités de facturation mais aussi le niveau de service garanti (SLA)[104] et les pénalités en cas de violation, ainsi que la durée et les modalités de résiliation.

La définition du périmètre des prestations fournies constitue un élément essentiel du contrat car il permet en premier lieu de définir les obligations du prestataire. Il constitue aussi la base de la qualification juridique du contrat et de la détermination de la rémunération[105].

Dans les projets *ad hoc,* contrairement aux solutions standards fournies en mode cloud, le périmètre est souvent source d'incompréhensions entre les parties et peut représenter un risque majeur si certaines prestations venaient à n'être prises en charge par aucune des parties[106], ou lorsque certaines prestations essentielles ne font pas partie du périmètre inclus dans la rémunération convenue. Un effort de rédaction important doit être entrepris afin que l'administration ne se retrouve pas dans l'obligation de payer des prestations essentielles qui seraient hors périmètre. Il peut être aussi utile d'anticiper et de négocier en amont la rémunération de ce qui est hors périmètre.

Par ailleurs, le mode de facturation doit être examiné avec attention, en particulier s'il s'agit d'un forfait, en prévoyant précisément ce qui est inclus, et en prévoyant s'il y a des limites ou un budget lorsqu'il s'agit d'un tarif horaire. Les conséquences du dépassement du nombre d'utilisateurs/utilisations doivent être particulièrement examinées. Idéalement, on devrait mettre à la charge du fournisseur une obligation d'information préalable, voire exiger de lui qu'il obtienne l'accord écrit de l'administration avant de pouvoir facturer tout ce qui dépasserait ce qui a été initialement prévu.

Lorsque l'accès aux services fournis par le prestataire se fait par le biais de l'octroi d'une licence, il faudra déterminer s'il s'agit d'une licence payée une seule fois (portant ou non sur les mises à jour) avec ou sans limite dans le temps et dans l'espace ou d'une licence renouvelable périodiquement. Si la licence est cédée contre le paiement de redevances périodiques, il faudra prendre garde aux limites qui peuvent y être liées (nombre d'utilisateurs, durée, etc.) aux obligations qui en découlent (renouvellement automatique, obligation d'annoncer les modifications dans l'utilisation, etc.). Il est utile de rappeler que si cette licence prend fin, elle n'empêche pas l'accès aux données de l'administration, ainsi que la transition qui aura été convenue dans le contrat. Si l'accès au code source est important, il faudra le préciser, et prévoir un moyen de l'obtenir en cas de disparition du prestataire.

Les contrats informatiques ont une particularité concernant la garantie pour les défauts. Il est communément admis qu'aucun logiciel ne peut être totalement exempt de tout dysfonctionnement, raison pour laquelle il est recommandé aux parties de définir objectivement les obligations du prestataire afin de pouvoir déterminer s'il y a conformité ou violation des obligations contractuelles[107]. Ces critères sont généralement intégrés dans des annexes au contrat principal, au travers de SLA. Leur but est de décrire de manière quantitative et objective la qualité de la prestation de services rendue[108]. En pratique, il n'y a souvent aucune garantie pour les défauts lorsqu'il s'agit d'un contrat de mandat, et une garantie limitée à 30 jours dans le cadre d'un contrat d'entreprise, obligeant ainsi indirectement l'administration à souscrire des prestations de maintenance.

Le niveau de service nécessaire dépendra de la sensibilité du projet et de la capacité pour l'administration à accepter une indisponibilité passagère. Il faudra préciser le seuil, objectivement évaluable et contrôlable par l'administration, en dessous duquel la prestation n'est pas

---

103 Art. 253 ss CO.

104 *Service-level agreement.*

105 Jaccard/Robert (n. 86), 107.

106 Un exemple classique est celui de la gestion des sauvegardes de données. Si l'administration croit que le fournisseur s'en charge et que le prestataire considère que cette prestation n'est pas dans le périmètre des prestations fournies, personne ne sauvegardera les données. En cas de problème, il y aura non seulement un litige pour déterminer qui en porte la responsabilité, mais peut être pire encore des données importantes pourraient ne jamais être récupérées.

107 Jaccard/Robert (n. 86), 108.

108 À ce sujet, Jacques De Werra, Les contrats de niveau de service, Internet 2005 : travaux des journées d'étude, Lausanne (CEDIDAC) 2005, 111 ss.

considérée comme délivrée correctement (par exemple une durée unique d'indisponibilité maximale, une durée moyenne d'indisponibilité, un taux d'erreurs, une vitesse de réponse, etc.).

La sanction de ces manquements doit être prévue, premièrement sous la forme de crédits[109] et deuxièmement par un droit de résiliation anticipé. En cas de manquement mineur (à définir dans le SLA), un remboursement proportionnel au manquement (et au montant facturé pour le service) sera prévu ; il est généralement déduit sur la facture suivante. On peut toutefois aussi imaginer qu'un remboursement en argent soit convenu, en particulier en cas de fin de contrat. Rien n'empêche les parties d'accepter que ce montant excède ce qui a été versé par l'administration, même si le fournisseur sera généralement peu enclin à l'accepter.

En cas de manquement important ou répété (il est recommandé de préciser également ces notions dans le contrat ou le SLA), il faudra prévoir un droit de résiliation anticipé, idéalement cumulé avec une indemnisation. L'idée ici est que si le fournisseur n'est pas à même, de façon répétée ou après avoir été averti, de fournir la prestation correctement, l'administration doit pouvoir mettre fin au contrat rapidement sans attendre l'échéance convenue. Le sort des montants déjà versés et une éventuelle indemnisation doivent également avoir été envisagés ainsi que le mode de dédommagement et la possibilité de l'administration de faire exécuter les prestations par un tiers aux frais et risques du prestataire.

Une correcte définition du périmètre et l'existence de SLA permettent de déterminer plus aisément et objectivement la réalisation de la condition de l'inexécution de l'obligation contractuelle du prestataire. En outre, les SLA ont pour effet de fixer par avance les conséquences financières de ces manquements[110]. Il est recommandé en pratique de prévoir l'émission par le prestataire informatique de notes de crédit que l'administration pourra faire valoir lorsque les niveaux de services imposés par les SLA ne sont pas atteints, ce qui contribue grandement à la mise en œuvre de la responsabilité du prestataire pour les défauts, tout en représentant une motivation supplémentaire pour ce dernier à fournir sa prestation dans le respect du contrat conclu[111].

[109] Les crédits SLA peuvent être convertis à une échéance convenue en un dédommagement financier ou un montant à déduire d'une facture future.

[110] De Werra (n. 108), 124.

[111] Jaccard/Robert (n. 86), 110.

D. La fin du contrat

Si la résiliation des contrats informatiques ponctuels soulève relativement peu de difficultés en pratique, ce n'est pas toujours le cas de qui régissent des projets informatiques de durée. En plus des modalités juridiques de résiliation, il est fondamental de prendre en compte dès la négociation du contrat les problèmes de transition (migration de données, accès aux codes sources, dépendance vis-à-vis d'un prestataire, etc.).

Il est ainsi essentiel de prévoir avant la signature du contrat les modalités pour y mettre fin mais également les conséquences de la fin du contrat et les obligations de réversibilité (assistance à la transition vers un nouveau prestataire). Selon la nature du service proposé, il sera important de s'assurer de la portabilité des informations, soit par l'engagement du fournisseur d'utiliser un format ouvert librement réutilisable, soit par l'engagement du fournisseur de fournir – y compris après la fin du contrat – les moyens nécessaires pour assurer la conversion et la transition vers un autre fournisseur de services, et parfois l'accès direct aux données, ce qui peut s'avérer particulièrement utile si le fournisseur ne veut ou ne peut honorer ses engagements liés à la transition.

V. Conclusions

De plus en plus de services sont fournis en mode cloud public. S'ils revêtent de nombreux avantages pour les entreprises privées, ils peuvent être un véritable casse-tête pour l'administration, surtout s'il n'y a pas d'alternative suisse.

Le traitement de données par un tiers est d'abord un cas de délégation de traitement au sens du droit de la protection des données. Un contrat est nécessaire, avec des garanties particulières, notamment de confidentialité et de sécurité. Ensuite, cela conduira le plus souvent à un traitement de données à l'étranger, ce qui nécessite aussi des garanties spécifiques. Si les données concernées sont soumises au secret de fonction (ce qui est généralement le cas des données traitées par l'administration), le secret de fonction s'opposera finalement purement et simplement à un traitement à l'étranger (sauf si les données sont chiffrées et que le fournisseur n'a pas la clé, mais cela n'est souvent techniquement pas possible).

Il est donc nécessaire de revoir, par la voie parlementaire ou prétorienne, la portée du secret de fonction et de donner à l'administration les moyens techniques de mener à bien ses tâches. Ne rien faire va obliger, à brève échéance, l'administration à développer des solutions internes (certainement coûteuses et peu efficientes) ou utiliser des services cloud en violation de la loi (qu'il s'agisse de *shadow IT* ou de projets officiels).