CHA/novembre 2019

RAPPORT EXPLICATIF

accompagnant l'avant-projet de loi adaptant la législation cantonale à certains aspects de la digitalisation

EN BREF

La digitalisation des prestations de l'administration cantonale fribourgeoise est un projet phare du programme gouvernemental du Conseil d'Etat pour la législature 2017–2021. Il s'agit d'un vaste chantier qui va transformer en profondeur l'administration et sa manière de fournir les prestations. La digitalisation des prestations entraîne autant des adaptations techniques que des évolutions dans la gestion des processus et au niveau des bases légales. Sur ce dernier plan, le Conseil d'Etat a opté pour une approche pragmatique et progressive en intégrant, dans la première loi adoptée dans ce domaine, la possibilité de travailler dans le cadre de projets pilotes. Ceux-ci permettent de mettre en place de nouvelles pratiques et d'en collecter les expériences avant de procéder définitivement aux adaptations législatives nécessaires.

Depuis l'entrée en vigueur de la loi sur le guichet de cyberadministration de l'Etat (LGCyb ; RSF 17.4), le Conseil d'Etat a autorisé, sur la base de son article 21, la réalisation de deux projets pilotes dans le domaine de la cyberadministration.

Le premier projet pilote concerne l'externalisation de certaines données dans le *cloud* qui a pour but de permettre à l'Etat d'utiliser les dernières avancées de la technologie tout en respectant les exigences de la protection des données. Ce projet est pour l'essentiel terminé. Le SITel a rendu son rapport d'évaluation au Conseil d'Etat dans le courant du mois de novembre. Celui-ci déclare un retour d'expérience suffisamment probant pour envisager l'adoption des bases légales nécessaires en vue d'étendre les possibilités de recours à des solutions de *cloud computing*.

Pour être en mesure de passer de la phase pilote à la phase de production du projet et d'étendre ainsi les possibilités de recourir à des solutions de *cloud computing*, il est nécessaire de quitter la phase pilote et de modifier la loi sur la protection des données (LPrD ; RSF 17.1) en vue d'y introduire les bases légales autorisant l'externalisation de données personnelles. Or, si l'avant-projet de révision totale de la LPrD va déjà dans ce sens, il est probable qu'il n'entrera pas en vigueur avant le 1er janvier 2021, voire 2022. Or un tel délai ralentirait sensiblement les travaux de mise en œuvre du plan directeur cantonal de la digitalisation et des systèmes d'information décidé par le Conseil d'Etat pour concrétiser son projet phare Fribourg 4.0. Le présent avant-projet prévoit donc de faire entrer en vigueur de manière anticipée les dispositions de l'avant-projet de révision totale de la LPrD relatives à cette question en les intégrant dans le texte actuel de la loi.

Le deuxième projet pilote décidé par le Conseil d'Etat n'est pas concerné par ces questions d'externalisation. Il s'agit de la mise en œuvre du Référentiel cantonal de personnes, organisations et nomenclatures. La phase pilote vient de démarrer, est donc toujours en cours et devrait se poursuivre jusqu'à l'été 2021. Néanmoins, il est ressorti des travaux menés jusqu'ici que le Référentiel cantonal ne pourra pas atteindre ses objectifs s'il n'est pas autorisé à traiter systématiquement le numéro AVS (NAVS) dans le but d'identifier de manière sûre et univoque les personnes recensées. Or le droit fédéral exige impérativement l'existence d'une base légale adoptée par le Grand Conseil pour permettre aux cantons d'utiliser le NAVS dans ce but.

L'utilisation systématique du NAVS est en discussion sur le plan fédéral. Le Conseil fédéral vient de confirmer le message y relatif. Mais, là aussi, les délais ne permettent pas d'espérer une mise en œuvre immédiate.

Pour permettre de résoudre rapidement ces deux situations, la Chancellerie d'Etat a préparé, en collaboration avec la Direction des finances, les bases légales nécessaires. Il a paru en outre souhaitable de profiter de ces travaux pour apporter certains compléments à la LGCyb en lien avec l'avancement des travaux relatifs à la digitalisation de l'administration.

1 GÉNÉRALITÉS

A la fin de l'année 2016, le Conseil d'Etat présentait au Grand Conseil son projet de loi sur le guichet de cyberadministration de l'Etat (LGCyb). L'objectif était de régler la création et la gestion d'un guichet virtuel unique, porte d'entrée vers les différents services de l'administration sur Internet, et de poser les prérequis techniques et les principes généraux de la cyberadministration cantonale.

Depuis, de nombreux travaux ont été menés dans le but de moderniser le canton, de rendre les opérations administratives plus aisées et plus économiques pour les administré-e-s et plus efficientes pour l'administration. Parmi ces travaux, certains ont été couronnés de succès : le canton de Fribourg s'est, par exemple, distingué sur la scène nationale en ayant développé la solution *Simple eSign* qui assure simultanément l'échange sécurisé de documents numériques et la signature électronique au moyen d'une solution unique, standardisée et conviviale[1]. Il est aussi le premier canton en Suisse à proposer la délivrance d'actes authentiques de l'état civil au format électronique.

La mise sur pied de cette nouvelle manière d'offrir les prestations et de construire le fonctionnement de l'Etat est un vaste projet qui nécessite de repenser fondamentalement la gestion des processus et la fourniture des prestations. L'architecture du guichet virtuel est conçue de manière que les services de base (identification, paiement, signature, sécurité, etc.) soient proposés une fois pour toutes de manière identique. Chaque nouvelle prestation offerte pourra ainsi s'appuyer sur ces services de base selon des critères clairement définis pour l'ensemble de l'Etat.

La LGCyb permet explicitement de travailler par l'entremise de projets pilotes décidés par le Conseil d'Etat afin de construire, pas à pas, la digitalisation de l'administration et de ne légiférer que lorsque les entités concernées ont pu tester et valider les enseignements de ces divers projets. Cette manière de travailler permet au canton de Fribourg d'avancer dans sa transformation numérique de manière aussi prudente et clairvoyante que possible.

Ainsi, le présent avant-projet permet de mettre déjà en œuvre les enseignements recueillis dans le cadre de deux projets pilotes conduits par le Conseil d'Etat depuis 2018. Il apporte également quelques adaptations ponctuelles de la LGCyb qui tirent les enseignements de sa première mouture et tiennent compte de certains changements survenus depuis son adoption. Il règle en particulier la question de l'externalisation de données et d'applications informatiques auprès de personnes extérieures à l'administration en dehors du contexte de la protection des données.

Avec les nouvelles dispositions proposées, la LGCyb présentera un contenu qui dépasse le cadre du seul guichet de cyberadministration. C'est pourquoi l'avant-projet propose de la renommer en loi sur la cyberadministration (LCyb).

[1] https://www.egovernment.ch/fr/umsetzung/innovationen/innovationen-20182019/.

2 CONTENU DE LA PRÉSENTE RÉVISION

L'avant-projet porte sur trois points qui sont tous en lien avec la stratégie menée par le Conseil d'Etat en matière de digitalisation. Il prévoit les bases légales nécessaires afin d'autoriser dans un cadre sécurisé l'externalisation de données auprès de personnes extérieures à l'administration (2.1) ; il permet au Référentiel cantonal de traiter systématiquement le NAVS aux fins d'identifier de manière sûre et univoque les personnes recensées (2.2) ; il apporte quelques adaptations ponctuelles relatives à certains aspects de la digitalisation (2.3).

2.1 Externalisation de données

Conformément à l'article 4 LPrD), les organes publics ne sont en droit de traiter des données personnelles que si une disposition légale le prévoit ou, à défaut, si les dispositions réglant l'accomplissement de leur tâche l'impliquent. La définition de ce qu'est un traitement de données apparaît à l'article 3 al. 1 let. d LPrD ; il s'agit de toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données.

Quand bien même la définition d'un traitement de données prévu dans la LPrD ne cite pas expressément le cas de l'externalisation, il est clair que ce type d'opération entre dans le champ d'application de la disposition. Aussi une base légale est-elle nécessaire afin de pouvoir externaliser des données, en particulier dans le *cloud* (pour la définition de l'externalisation, voir l'article 2 al. 1 let. g LCyb tel qu'introduit par le projet et les commentaires y relatifs).

Le recours à l'externalisation et plus particulièrement au *cloud* constitue une réponse à des exigences nouvelles dans le fonctionnement et l'organisation de l'Etat, qui résultent du déploiement des technologies numériques dans la société : explosion des volumes de données produites et utilisées, exigences de haute disponibilité et de sécurité, volonté des organes de l'Etat de se concentrer sur le cœur de leur activité et de se désengager de certaines opérations qui ne correspondent pas à leur métier, besoins de nouveaux moyens d'accès aux services en situation de mobilité, en tout lieu, à tout moment et sur tout support.

Il est vrai cependant que l'utilisation de tels services requiert la prise de précautions adaptées aux circonstances et aux risques engendrés. C'est pourquoi, avant d'autoriser plus largement l'externalisation de données, le Conseil d'Etat a commencé par réaliser à partir de la fin de l'année 2018 un projet pilote portant sur l'externalisation de données personnelles dans quatre solutions *cloud* (cf. ordonnance du 4 décembre 2018 autorisant le Service de l'informatique et des télécommunications à externaliser le traitement de certaines données dans le « Cloud » [projet pilote] ; [RSF 17.42]). Les résultats du projet portant spécifiquement sur la solution « outils bureautiques collaboratifs » Microsoft 365 ont fait l'objet d'un rapport d'évaluation qui a été transmis au Conseil d'Etat au mois de novembre 2019. Celui-ci conclut et souligne que les exigences envers les trois autres solutions « Cloud » autorisées par l'ordonnance sur les projets « Cloud » constituent un sous-ensemble des exigences formulées à l'égard de Microsoft 365 et, par conséquent, qu'elles peuvent s'appliquer également aux autres solutions. Ainsi, sur la base des expériences acquises avec la solution Microsoft 365, le Conseil d'Etat considère qu'il dispose de suffisamment de retours probants pour proposer au Grand Conseil l'adoption des bases légales formelles nécessaires permettant l'externalisation du traitement de données personnelles, y compris sensibles, dans le *cloud*.

Tenant compte des expériences menées durant la phase pilote, les articles 13b et 18 prévus par l'avant-projet créent un cadre juridique à même de soutenir l'utilisation de ces nouveaux outils au sein de l'Etat dans un environnement le plus adapté et le plus sécurisé possible. Les mesures de sécurité prévues reprennent en particulier les recommandations de la Conférence des préposé-e-s suisses à la protection des données (PRIVATIM)[2]. Pour pouvoir procéder à une externalisation, les mesures suivantes devront notamment être respectées :

> les lieux de traitement doivent être situés en tout temps sur le territoire suisse ou sur le territoire d'un Etat garantissant un niveau de protection équivalent[3] ;

> le mandataire doit être choisi avec soin et la protection des données, assurée par la conclusion d'un contrat systématique et circonstancié ;

> la confidentialité des données faisant l'objet d'une obligation légale ou contractuelle de garder le secret doit être garantie, y compris à l'égard du mandataire ;

> les données externalisées doivent pouvoir être récupérées dans le but de changer de mandataire ou de procéder à leur ré-internalisation.

La formulation des articles 13b et 18 est identique à celle des articles 20 et 37 de l'avant-projet de révision totale de la LPRD mis en consultation en parallèle au présent avant-projet de loi.

Comme il semblerait illogique que l'Etat puisse externaliser seulement des données personnelles à l'exclusion de tout autre type de données, le Conseil d'Etat propose également des dispositions concernant l'externalisation de données et d'applications informatives hors du champ d'application de la LPrD (art. 21 à 21c). Dans le but de faire en sorte que l'Etat conserve la maîtrise de son patrimoine informationnel et applicatif, la réglementation proposée prévoit la prise de mesures organisationnelles et techniques similaires à celles qui concernent l'externalisation de données personnelles.

2.2 Utilisation systématique du numéro AVS par le Référentiel cantonal

Le 24 juin 2019, le Conseil d'Etat a adopté, en se fondant sur l'article 21 LGCyb, une ordonnance expérimentale concernant la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures (projet pilote) (RSF 17.45). Cette ordonnance est destinée à mettre en œuvre les articles 13 al. 1 let. b, 15 et 16 LGCyb qui prévoient la création d'une plate-forme informatique gérant un référentiel des personnes et des données de base. Elle sera remplacée au terme de la phase pilote par une loi au sens formel, distincte de la LGCyb. La loi en question contiendra des bases légales précises et circonstanciées concernant l'organisation et le fonctionnement de cette nouvelle infrastructure numérique appelée à jouer un rôle central à l'échelon cantonal.

Le but du Référentiel cantonal est de fournir aux différents organes de l'Etat certaines données de référence qui soient autant que possible complètes, exactes et à jour. Pour des raisons évidentes de protection des données, les données contenues dans le Référentiel cantonal ne sont néanmoins pas mises librement à la disposition des organes de l'Etat selon leur bon vouloir. Le système est conçu pour garantir la segmentation des données à travers diverses approches de granularité en termes d'accès, de périmètre et de profondeur des données. Avant d'accéder aux données du Référentiel cantonal, les organes publics doivent conclure préalablement une convention qui détermine, conformément à

[2] PRIVATIM, *Aide-mémoire « Risques et mesures spécifiques à la technologie de Cloud computing »*, version 1.0 du 6 février 2019. Texte disponible à l'adresse : http://www.privatim.ch/wp-content/uploads/2019/03/ privatim_Aide-memoire_Cloud_v1.0_20190206.pdf.

[3] Cette exigence s'aligne sur le droit européen. En principe, les Etats qui y satisfont sont ceux qui sont soumis au droit européen de la protection des données ou qui sont au bénéfice d'une décision d'adéquation dans ce domaine rendue par la Commission européenne.

la législation en vigueur, l'étendue de leurs droits d'accès et les obligations qu'ils sont tenus de respecter, en particulier sous l'angle de la sécurité.

Lorsqu'il a proposé le projet de LGCyb en 2016, le Conseil d'Etat avait renoncé à utiliser systématiquement le NAVS comme identificateur de personnes, préférant créer à la place un numéro d'identification cantonal. Aussi bien l'objectif de création que l'utilisation d'un nouvel identifiant cantonal distinct du NAVS sont maintenus et au centre des mécanismes prévus. Toutefois, les besoins et expériences menées à ce jour ont montré la nécessité de ne pas exclure l'utilisation du NAVS dans des situations spécifiques. Le NAVS permet notamment de régler convenablement la plupart des problèmes d'arbitrage liés à l'identification des personnes ou résultant d'informations manquantes ou incohérentes. Le NAVS est par ailleurs essentiel pour certains échanges de données avec d'autres autorités, notamment celles qui sont situées hors du canton de Fribourg. L'avant-projet propose dès lors d'autoriser le Référentiel cantonal à utiliser systématiquement le NAVS dans le but d'identifier de manière sûre et univoque les personnes recensées. Les dispositions prévues dans ce but répondent aux exigences de l'article 50e al. 3 de la loi du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS ; RS 831.10) concernant l'utilisation du NAVS par les cantons en dehors du champ des assurances sociales.

A noter que l'avant-projet ne se limite pas simplement à autoriser le Référentiel cantonal à utiliser systématiquement le NAVS. Il prévoit au surplus de nombreuses cautèles dans le but de prévenir toute utilisation abusive de celui-ci. En particulier, le NAVS ne pourra aucunement être utilisé comme moyen d'apparier des données entre elles afin d'évaluer certaines caractéristiques personnelles des citoyens et citoyennes ou de mener des investigations dans le but d'identifier des individus en situation d'irrégularité. Une telle utilisation du NAVS et du Référentiel cantonal nécessiterait obligatoirement l'adoption d'une loi spéciale par le Grand Conseil. D'autres mesures techniques sont aussi prévues, qui sont décrites plus en détail dans les commentaires des dispositions pertinentes. Il convient également de rappeler que, sur le plan organisationnel, l'Autorité cantonale de la transparence et de la protection des données (ATPrD) est régulièrement consultée lors des travaux de mise en œuvre du Référentiel cantonal et peut en tout temps procéder à des audits.

Cette ouverture liée à l'utilisation du NAVS fait écho aux discussions actuellement en cours sur le plan fédéral qui prévoient également l'élargissement des possibilités d'utilisation du NAVS, moyennant le respect de conditions strictement définies. L'utilisation du NAVS en tant que caractéristique d'identification des personnes est par ailleurs nécessaire dans le cadre de projets phares de la Confédération, tels le projet *e-déménagement* ou celui du Service National d'Adresses auquel le Référentiel cantonal prévoit de s'interconnecter.

2.3 Autres modifications

L'avant-projet profite de la présente révision pour apporter des modifications ponctuelles dans la LGCyb, qui précisent certains aspects liés au fonctionnement du guichet virtuel, notamment :

> il introduit l'exigence du consentement libre et éclairé de la personne concernée afin que le guichet virtuel puisse collecter les données personnelles nécessaires à la délivrance de la prestation ou du service requis et les transmette au service compétent pour traiter sa demande ;

> il introduit également le principe de la protection des données par défaut (*privacy by default*) dans le fonctionnement du guichet virtuel, tout en réservant les possibilités pour les usagers et usagères de consentir à un traitement élargi de leurs données ;

> il permet au Conseil d'Etat d'adhérer à des organisations intercantonales spécialisées dans le domaine de la cyberadministration en lien avec le guichet virtuel et formalise dans ce cadre la participation du canton Fribourg à l'association iGovPortal.ch (cf. pt 8.5 ci-dessous).

3 DÉROULEMENT DES TRAVAUX

Durant l'automne 2019, la Chancellerie d'Etat, avec l'appui de la Direction des finances (DFIN), a constitué un groupe de travail en vue d'adapter la législation cantonale à certains aspects de la digitalisation. Celui-ci était composé d'une représentante de la DFIN, de la préposée à la protection des données et de représentants du Service de législation.

L'objectif était, d'une part, de permettre de passer de la phase pilote à la phase de production dans le cadre du projet concernant l'externalisation du traitement de certaines données dans le *cloud* et, d'autre part, de tenir compte des enseignements déjà tirés relatifs au projet pilote concernant la mise en œuvre du Référentiel cantonal de personnes, organisations et nomenclatures. Les travaux menés par le groupe de travail ont permis de mettre en évidence d'autres besoins d'adaptation ponctuels, notamment concernant le fonctionnement du guichet virtuel et l'externalisation de données et d'applications informatiques hors du contexte de la protection des données.

4 IMPACT FINANCIER ET EN PERSONNEL DE LA PRÉSENTE RÉVISION

En fixant un cadre légal à l'externalisation de données, l'avant-projet n'entraîne pas de nouvelles dépenses ni de besoins nouveaux en personnel. Les dépenses qui résulteront de l'externalisation de données ou d'applications informatiques dépendront des futurs projets qui seront décidés dans ce domaine par les organes compétents.

5 CONFORMITÉ AU DROIT SUPÉRIEUR

L'avant-projet traite de questions d'ordre organisationnel et de protection des données qui relèvent principalement du droit cantonal. Dans ces domaines, il convient en particulier de prendre en considération l'article 12 al. 2 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst.) qui garantit le droit à la protection des données personnelles et aussi l'article 54 qui traite de la question de la délégation de tâches publiques à des tiers. L'avant-projet prévoit toute une série de mesures visant à garantir le respect de ces deux dispositions.

L'avant-projet traite aussi de la question de l'utilisation systématique du NAVS dans le cadre du Référentiel cantonal. Les conditions d'une telle utilisation par les cantons en dehors du domaine des assurances sociales sont fixées à l'article 50e al. 3 de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS). Les dispositions de l'avant-projet sont conformes aux exigences du droit fédéral.

6 AVIS DE L'AUTORITÉ DE LA TRANSPARENCE ET DE LA PROTECTION DES DONNÉES (ATPrD)

Durant les travaux préparatoires, l'ATPrD a indiqué qu'elle n'était pas favorable à l'idée de faire entrer de manière anticipée les dispositions concernant l'externalisation de données personnelles, sans y être opposée sur le fond. En effet, elle estime qu'il n'est pas opportun de « saucissonner » l'avant-projet de révision de la LPrD, que celui-ci forme un tout et qu'il n'y a aucune raison de faire entrer de manière anticipée certaines des dispositions qu'il contient, ce d'autant que l'avant-projet de révision de la LPrD est prêt à partir en consultation et qu'il groupe toutes les dispositions traitant des standards de protection adaptés et nécessaires à une externalisation.

S'agissant de l'utilisation systématique du NAVS dans le cadre du Référentiel cantonal, l'ATPrD n'a jamais caché son scepticisme face à ce thème, et ce même si les possibilités d'une telle utilisation du NAVS venaient à être élargies lors d'une révision de la LAVS. Comme cela a déjà été mentionné plus haut, le Conseil fédéral a cependant adopté, le 30 octobre 2019, un projet de modification de la LAVS concernant l'utilisation systématique du NAVS. Selon ce projet, les cantons pourront utiliser

systématiquement le NAVS sans qu'il soit nécessaire d'adopter pour cela une base légale spécifique. Ainsi, même si les présentes dispositions n'étaient pas adoptées, il est probable que le Référentiel cantonal pourra de toute manière traiter le NAVS dans un délai d'une année à deux ans. Un tel délai ralentirait cependant considérablement les travaux de mise en œuvre du Référentiel cantonal, ce qui aurait un impact non négligeable sur le fonctionnement de l'administration ainsi qu'en termes de coûts.

7 ADAPTATIONS DE LA LPrD – Commentaires

7.1 Art. 13b – Externalisation

Dans le domaine des systèmes d'information, l'externalisation de certains services auprès de prestataires tiers est devenue une pratique incontournable, aussi bien pour les entreprises du secteur privé que pour les administrations publiques. Les entreprises du secteur des technologies de l'information et de la communication disposent en effet de ressources et de compétences hautement spécialisées en termes de qualité des prestations, de performance, de capacité d'innovation ou encore de sécurité qui dépassent ce que l'Etat peut lui-même fournir dans ce domaine.

Le projet pilote mené par le SITel concernant l'externalisation de certaines données dans le *cloud* a déjà permis d'explorer les possibilités techniques dans ce domaine et aussi d'approfondir les aspects sécuritaires afin de s'assurer de l'adéquation de ce type de solution avec les exigences légales en matière de protection des données. La présente disposition fait en sorte d'autoriser le recours à des solutions de *cloud computing* dans un cadre délimité et sécurisé correspondant aux standards les plus élevés dans ce domaine. A noter que cette ouverture correspond à l'un des objectifs du « Catalogue de mesures pour la stratégie d'informatique en nuages des autorités suisses 2012–2020 » (Orientation O2 : Adaptation des bases légales)[4].

Des exigences particulières sont fixées pour permettre aux organes publics à la fois de conserver la maîtrise des données externalisées et de garantir la protection des droits des personnes. Avant toute chose, l'alinéa 1 spécifie que le fournisseur de services est considéré comme un mandataire ; cela signifie que l'organe qui externalise des données reste entièrement responsable de leur traitement. Il doit donc prendre toutes les mesures et les précautions nécessaires pour que l'externalisation se passe sans heurts. En outre, l'organe externalisant doit s'assurer que les lieux d'hébergement des données sont situés en permanence en Suisse ou sur le territoire d'un Etat disposant d'une législation équivalant à la LPrD (al. 2). Sont visés ici en particulier les Etats membres de l'Union européenne, dont la législation en matière de protection des données est, depuis l'entrée en vigueur du Règlement général (UE) 2016/679 sur la protection des données, la plus restrictive au monde.

A noter que ces exigences, auxquelles s'ajoutent celles de l'article 18 de l'avant-projet (traitement sur mandat), reprennent largement les recommandations de la Conférence des préposé-e-s suisses à la protection des données en matière d'externalisation[5].

Conformément à l'alinéa 4, le Conseil d'Etat précisera, par voie d'ordonnance ou réglementaire, les exigences spécifiques destinées à garantir le niveau de protection le plus élevé possible, notamment en termes de choix et de contrôle du mandataire. Dans un souci de transparence, il publiera également une liste sur Internet des mandataires auprès desquels il procède à des externalisations.

[4] https://www.egovernment.ch/files/8814/5398/6362/Katalog-f.pdf.
[5] PRIVATIM, Aide-mémoire « *Risques et mesures spécifiques à la technologie de Cloud computing*» (document disponible à l'adresse Internet : http://www.privatim.ch/wp-content/uploads/2019/03/privatim_Aide-memoire_Cloud_v1.0_20190206.pdf).

7.2 Art. 18 – Traitement sur mandat

L'article 18 règle les questions de responsabilité lorsqu'un organe public fait appel à la collaboration de personnes privées afin de traiter des données personnelles (traitement sur mandat). Les opérations de traitement qui sont confiées à une entreprise sous-traitante peuvent soit se dérouler directement dans le périmètre d'activité du responsable du traitement, ce qui suppose que l'entreprise sous-traitante utilise le matériel informatique de l'Etat, soit être entièrement externalisées sur les infrastructures et les systèmes informatiques de l'entreprise, auquel cas on appliquera en sus l'article 13b sur l'externalisation de données.

Alinéa 1 – La disposition rappelle que la protection et la sécurité des données qui sont traitées pour le compte d'un organe de l'Etat par une entreprise tierce doivent être garanties comme si le traitement était réalisé par l'organe lui-même (qui demeure seul responsable de la protection des données traitées).

Alinéa 2 – Conformément à cette disposition, les données soumises à une obligation légale ou contractuelle de garder le secret peuvent être confiées à un mandataire uniquement si la confidentialité est garantie non seulement à l'égard des tiers mais également à l'égard du mandataire lui-même. C'est le cas en particulier si les données transmises ont été chiffrées et que le mandataire ne dispose pas de la clé de déchiffrement.

Alinéa 3 – La disposition interdit au mandataire de sous-traiter des données auprès d'un tiers sans l'accord préalable du responsable du fichier. Comme le mandataire n'est en principe pas directement soumis à la législation cantonale, cette précaution devra figurer dans le contrat de mandat.

8 ADAPTATIONS DE LA LGCyb – Commentaires

8.1 Art. 2 – Terminologie

La disposition est complétée par l'ajout de deux nouvelles définitions :

a) La définition donnée de la « cyberadministration » correspond, sous une forme succincte, à celles qui sont retenues dans les stratégies suisse[6] et fribourgeoise[7] de cyberadministration. Elle sert à mettre en évidence le fait que la cyberadministration ne concerne pas uniquement la fourniture de prestations à la population sous forme électronique (*front office*) mais qu'elle englobe aussi les changements apportés concernant l'organisation et le fonctionnement interne de l'Etat (*back office*).

b) L'institutionnalisation du terme « externalisation » dans la législation cantonale correspond à une réalité qui concerne non seulement le canton de Fribourg mais également la quasi-totalité des organisations publiques et privées en Suisse. Contrairement à une idée reçue, l'externalisation n'est pas une stratégie de réduction de la puissance publique et du périmètre de l'Etat mais correspond davantage à un réajustement de sa place dans une société elle-même en mutation. Dès l'instant où personne ne conteste l'existence de ce changement, la question n'est dès lors pas tant de savoir si celui-ci est bon ou mauvais, mais plutôt de chercher à l'encadrer et à le maîtriser du mieux possible. C'est dans ce but que l'avant-projet propose des bases légales claires et circonstanciées dans ce domaine.

[6] Stratégie suisse de cyberadministration du 1er mai 2017, p. 2 (document disponible à l'adresse Internet : https://www.egovernment.ch/files/6014/8361/7687/Stratgie-suisse-de-cyberadministration.pdf.

[7] Stratégie de cyberadministration de l'Etat de Fribourg du 2 décembre 2014, p. 4 (document disponible à l'adresse Internet : https://www.fr.ch/sites/default/files/contens/cha/_www/files/pdf70/fr_DIV_strategie_ cyberadministration_web.pdf.

8.2 Art. 3a – Traitements de données personnelles

Alinéa 1 – Le but premier du guichet de cyberadministration est de fournir aux administré-e-s des prestations et des services identiques à ceux qui sont proposés au guichet physique d'une administration mais sous forme électronique, depuis un guichet en ligne unique, accessible 24 heures sur 24, 7 jours sur 7.

Dans la mesure où les lois spéciales qui autorisent le traitement de données personnelles ne valent que pour les organes de l'Etat auxquels ces lois font référence, le guichet de cyberadministration ne peut pas s'en prévaloir pour traiter les données nécessaires à la délivrance de la prestation ou du service requis. C'est pourquoi il est demandé à la personne de donner son consentement pour que le guichet de cyberadministration puisse collecter auprès d'elle les données nécessaires au traitement de sa demande et les communiquer à l'organe compétent pour y donner suite.

La disposition indique les conditions de validité du consentement qui doit en particulier être libre et éclairé.

Dans le contexte du guichet de cyberadministration, la condition du consentement libre signifie que la personne qui refuserait un certain traitement de données ne peut pas se voir imputer un désagrément autre que celui d'avoir à se rendre au guichet physique pour déposer sa demande ou de l'adresser par courrier écrit. On réservera toutefois les cas où la loi impose la tenue de certaines procédures au format électronique, comme c'est le cas par exemple aujourd'hui pour les demandes de permis de construire qui sont traitées au moyen de l'application FRIAC (cf. art. 135a de la loi du 2 décembre 2008 sur l'aménagement du territoire et les constructions [LATeC ; RSF 710.1]).

Quant au caractère éclairé du consentement, il est en principe satisfait lorsque la personne est informée des organes de l'Etat et des éventuels prestataires tiers participant à la délivrance de la prestation ou du service requis, des données qui sont transmises dans ce cadre et des finalités des traitements effectués.

Alinéa 2 – La disposition indique que le consentement est une décision réversible et que la personne concernée conserve ainsi le contrôle sur l'utilisation de ses données.

Alinéa 3 – Dans le cadre de la délivrance de prestations ou de services sous forme électronique, le guichet virtuel se limite à assurer le rôle de passerelle entre la population et les organes compétents de l'Etat. C'est pourquoi il n'a en principe pas de raison de conserver les données plus longtemps que le temps nécessaire au traitement de la demande de l'usager ou de l'usagère. La question de la durée de conservation des données par le guichet virtuel est réglée actuellement à l'article 8 de l'ordonnance du 15 mai 2017 sur le guichet de cyberadministration de l'Etat (OGCyb ; RSF 17.41). En se chargeant de régler les détails, le Conseil d'Etat pourra permettre également que des prestations répondant à un besoin transversal de l'administration et à des exigences de conservation plus étendues puissent être proposées.

8.3 Art. 4 al. 1 – Frais et émoluments

La modification introduite vise à affirmer le caractère gratuit de l'accès au guichet de cyberadministration, quel que soit le moyen utilisé pour ce faire.

8.4 Art. 9a – Protection des données par défaut et consentement

Alinéa 1 – La disposition introduit le principe de la protection des données par défaut dans le fonctionnement du guichet de cyberadministration. Selon ce principe, qui constitue dorénavant l'un des piliers du droit de la protection des données, l'architecture technique du guichet de cyberadministration et les applications qu'il supporte doivent par défaut être configurées afin d'assurer le niveau de protection des données le plus élevé.

Alinéa 2 – Conformément à son droit à l'autodétermination informationnelle, la personne concernée doit conserver le plus possible la maîtrise des données la concernant et être en mesure de décider des usages possibles de celles-ci. Cela inclut en particulier le droit pour elle de consentir à un traitement élargi de ses données si elle y voit un intérêt particulier. Elle peut dans ce sens accepter l'utilisation de *cookies* informatiques en vue d'améliorer les performances et le fonctionnement du guichet virtuel, participer à un sondage en ligne ou encore s'inscrire à une *newsletter* dans le but de recevoir périodiquement des informations sur un thème qui l'intéresse. La présente disposition confère une assise juridique à ce type de traitements de données qui ne reposent pas sur l'existence d'une base légale spécifique.

En outre, l'avancement de la cyberadministration et des projets liés permettra progressivement d'accroître les domaines pour lesquels les citoyens et citoyennes pourront facultativement et de manière éclairée donner leur consentement par le biais d'interfaces spécialement créées en vue de la délivrance des prestations mises à leur disposition depuis le guichet virtuel. On peut penser notamment que la mise en œuvre du droit d'accès prévu dans la LPrD, telles les habilitations accordées sur les données de la personne concernée, pourra un jour être associée à ces démarches participatives par le biais du guichet virtuel.

8.5 Art. 9b – Participation à des organisations intercantonales

Contrairement aux administrations d'autres pays qui fonctionnent de manière centralisée, la Suisse est un Etat fédéral qui compte 27 administrations (la Confédération et les 26 cantons). Cela implique souvent qu'une même solution est développée en interne 27 fois et que les coûts de production sont par conséquent multipliés par autant à l'échelle de la Suisse.

Pour réduire les coûts de production et aussi partager et profiter des expériences des autres cantons, le canton de Fribourg a développé des partenariats dans le domaine de la cyberadministration. Il a en particulier créé en 2017 l'association intercantonale iGovPortal.ch avec la République et canton du Jura. Cette association, qu'ont rejointe le canton de Soleure et celui de Saint-Gall depuis, met à la disposition de ses membres le code source, le code objet ainsi que la documentation technique pour la création complète d'un guichet virtuel de cyberadministration doté d'un large catalogue de prestations. En contrepartie, chaque membre s'engage à mettre à la disposition de tous les améliorations et les nouvelles applications qu'il développe lui-même à partir de la solution de base. L'association IGovPortal.ch permet de la sorte de mutualiser les efforts et les coûts de développement supportés par le canton dans le domaine de la cyberadministration.

La disposition confère une assise juridique à la participation du canton à l'association iGovPortal.ch et permet au Conseil d'Etat de rejoindre d'autres types d'organisations actives dans le développement de solutions relatives à la fourniture de prestations sous forme électronique. La participation des cantons à des organisations intercantonales est expressément encouragée à l'article 48 de la Constitution fédérale de la Confédération suisse du 18 avril 1999.

8.6 Art. 15 al. 1 let. h1 – Référentiel des personnes physiques

Les identificateurs sectoriels sont des identifiants dont l'utilisation est limitée localement à un secteur d'activité de l'Etat. Quand on utilise un identificateur sectoriel, les registres de ce secteur ne peuvent être reliés directement aux registres d'autres secteurs. En conséquence, si on recourt à des identificateurs sectoriels en respectant certains principes évoqués plus bas (cf. pts 6.7 et 6.8 ci-dessous), on réduit le risque qu'un attaquant n'agrège les données personnelles conservées dans chacun de ces registres, révélant ainsi des pans importants de la vie des individus concernés[8].

Pour pouvoir fonctionner, le Référentiel cantonal doit être en mesure de traiter les identifiants sectoriels de différents domaines d'activité de l'Etat, mais aussi des communes et, dans la mesure où le droit fédéral l'autorise, de la Confédération. Cela permet de faire le lien avec les autres systèmes d'information qui lui communiquent des données et ainsi d'identifier de manière sûre et univoque les personnes recensées. La modification proposée confère l'assise juridique nécessaire à cette fin.

8.7 Art. 15a – Utilisation systématique du numéro AVS – Principe

L'utilisation du NAVS par les cantons en dehors du champ d'application des assurances sociales est réglée à l'article 50e al. 3 LAVS. Selon cette disposition, l'utilisation du NAVS requiert l'adoption d'une base légale circonstanciée, dans une loi adoptée par le Grand Conseil, indiquant le but de l'utilisation et les organes légitimés à traiter le NAVS. Conformément à la disposition proposée, le Référentiel cantonal est habilité à traiter systématiquement le NAVS dans le but d'identifier de manière sûre et univoque les personnes recensées, de corriger les divergences et les incohérences constatées sur les données conservées (mauvaise orthographe, données inexactes ou données devenues obsolètes, etc.) et de procéder automatiquement aux changements qui sont annoncés auprès d'un organe de l'Etat (notamment, changement d'adresse ou changement d'état civil). Cet objectif vise en particulier à satisfaire au principe d'exactitude des données ancré à l'article 7 LPrD.

8.8 Art. 15a – Utilisation systématique du numéro AVS – Mesures de sécurité

Le Référentiel cantonal est hébergé sur les infrastructures informatiques de l'Etat. Il n'est pas concerné par une externalisation dans le *cloud*. Nécessaire au bon fonctionnement de l'Etat, l'utilisation systématique du NAVS comme identificateur de personnes n'en constitue pas moins un traitement de données personnelles qui doit offrir toutes les garanties de sécurité aux administré-e-s. C'est pourquoi des mesures techniques et organisationnelles sont indispensables afin d'encadrer son utilisation.

Les mesures prévues à l'article 15a de l'avant-projet correspondent aux standards internationaux les plus élevés concernant la sécurité des systèmes d'information de données personnelles. Elles reprennent en particulier les recommandations faites par le professeur David Basin de l'Ecole polytechnique fédérale de Zurich dans le rapport qu'il a rédigé sur la question à la demande conjointe de l'Office fédéral de la justice et du préposé fédéral à la protection des données.

Conformément à l'alinéa 1, le NAVS ne sera pas stocké dans le même registre que les autres données à caractère personnel mais dans un registre à part, contenant uniquement le NAVS et des identifiants sectoriels permettant, au moyen d'une table de liens tenue secrète, de mettre en relation des individus clairement identifiés avec leurs données personnelles.

Il est prévu d'appliquer en plus d'autres mesures techniques et organisationnelles, comme une délimitation claire des droits d'accès, la sensibilisation et la formation des personnes autorisées ainsi que

[8] BASIN David, *Risk Analysis on Different Usages of the Swiss AHV Number – Evaluation on behalf of the Federal Office of Justice and the Federal Data Protection and Information Commissioner*, septembre 2017, p. 26.

le recours à des technologies de cryptage des données. La prise de telles mesures est expressément exigée à l'alinéa 2 de la disposition.

8.9 Art. 16a et 16b – Utilisation systématique du numéro IDE et REE

L'équivalent du NAVS en Suisse comme identificateur de personnes pour les personnes morales sont le numéro d'identification des entreprises (IDE) et le numéro d'enregistrement non significatif (REE).

L'utilisation de ces identifiants est réglée à l'article 10 al. 3 de la loi fédérale du 9 octobre 1992 sur la statistique fédérale (LSF ; RS 431.01)[9] et dans la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE ; RS 431.03). Leur but est en particulier d'« identifier les entreprises de manière univoque, afin de simplifier et de sécuriser les échanges d'informations dans les processus administratifs et les travaux statistiques » (art. 1 LIDE).

Les articles 16a et 16b de l'avant-projet prévoient une réglementation analogue à celle qui concerne l'utilisation systématique du NAVS, mais sous une forme légèrement allégée compte tenu des risques moins élevés dans ce domaine.

8.10 Section 3.3, art. 21a, 21b et 21c – Externalisation

Dès lors que la loi autorise l'externalisation de données à caractère personnel, cela doit valoir aussi pour les données non personnelles ou des applications informatiques. Les dispositions de cette nouvelle section de la LGCyb sont à considérer comme des règles d'organisation importantes de l'administration, ce qui justifie leur insertion au niveau de la loi. Elles prévoient un cadre légal similaire à celui qui est prévu pour l'externalisation de données personnelles.

8.10.1 Art. 21a – Principes

La disposition introduit le principe selon lequel des données et des applications informatiques peuvent être externalisées auprès de personnes extérieures à l'administration (al. 1). Le terme de personne doit se comprendre au sens large ; il englobe les entreprises spécialisées dont l'externalisation et toutes les obligations qui en découlent relèvent de leur cœur de métier. Il ne s'agit toutefois pas d'une autorisation permettant aux organes de l'Etat d'externaliser tous azimuts leur patrimoine informationnel et applicatif auprès de tiers mais d'un principe organisationnel dont la mise en œuvre est spécifiée dans les dispositions qui suivent. C'est pour cette raison que la disposition réserve expressément la question du traitement de données personnelles, qui est régie par la législation sur la protection des données, ainsi que celle qui a trait à l'externalisation de tâches publiques, pour laquelle la Constitution cantonale exige l'adoption d'une base légale spécifique (al. 2).

8.10.2 Art. 21b – Mesures de sécurité

La disposition décrit les exigences sécuritaires à prendre en cas d'externalisation de données ou d'applications informatiques. Ces exigences qui ont fait leur preuve correspondent à celles que le Grand Conseil avait déjà prévues au moment d'autoriser l'externalisation des données de la banque de données de la législation fribourgeoise (cf. art. 8b de la loi du 16 octobre 2001 sur la publication des actes législatifs [LPAL ; RSF 124.1]).

[9] La disposition est complétée par l'ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements (OREE ; RS 431.903).

8.10.3 Art. 21c – **Responsabilité**

La disposition prévoit le même degré d'exigence en matière de responsabilité que celui qui est prévu pour l'externalisation de données personnelles (cf. art. 18 LPrD tel qu'introduit par l'avant-projet).
