# Message 2023-CE-149

26 juin 2023

—

accompagnant le projet de loi sur la protection des données (révision totale)

## Table des matières

—

**En bref** **3**

**1 Généralités** **4**

**1.1 Contexte et origine du projet** **4**

**1.2 Déroulement des travaux** **5**

**1.3 Grandes lignes du-projet** **6**

1.3.1 Contenu en général 6

1.3.2 Liens avec le droit de l'Union européenne et la Convention STE 108 modernisée 7

1.3.3 Droits des personnes concernées 8

1.3.4 Obligations des responsables du traitement 9

1.3.5 Autorité de surveillance en matière de protection des données 10

**1.4 Changements apportés suite à la consultation de 2019** **10**

**1.5 Conséquences du projet** **11**

**1.6 Conformité au droit supérieur et développement durable** **12**

**2 Commentaire des dispositions** **13**

**2.1 Section 1, Dispositions générales** **13**

**2.2 Section 2, Principes régissant le traitement de données personnelles** **16**

2.2.1 Section 2.1 : Conditions générales de licéité du traitement 16

2.2.2 Section 2.2 : Conditions supplémentaires applicables à certaines formes de traitement 18

2.2.3 Section 2.3 : Traitement de données à des fins ne se rapportant pas à la personne 25

**2.3 Section 3, Droits de la personne concernée** **25**

**2.4 Section 4, Mise en œuvre de la protection des données** **27**

**2.5 Section 5, Surveillance** **31**

2.5.1 Section 5.1 : Autorité de surveillance en matière de protection des données 31

2.5.2 Section 5.2 : Pouvoir de contrôle et d'intervention de l'Autorité de surveillance 34

**2.6 Section 6, Dispositions transitoires 35**
**2.7 Modification d'autres lois 36**
2.7.1 Adaptation de la LStat 36
2.7.2 Adaptation de la LOCEA 36
2.7.3 Adaptation de la LJ 36
2.7.4 Adaptation de la LCo 37
2.7.5 Adaptation du CPJA 37
2.7.6 Adaptation de la LVid 38
2.7.7 Adaptation de la LInf 38
2.7.8 Adaptation de la LMéd 38
2.7.9 Adaptation de la LCyb 38
2.7.10 Adaptation de la LS 39
2.7.11 Adaptation de la LESS 39
2.7.12 Adaptation de la LFE 39
2.7.13 Adaptation de la LSan 42
**3 Liste des principales abréviations 42**
**3.1 Actes législatifs 42**
**3.2 Autres abréviations 44**

## En bref

1. La loi actuelle sur la protection des données (LPrD) date du 25 novembre 1994. A cette époque, le *World Wide Web* venait d'éclore, *Google, Facebook, Twitter* et consorts n'existaient pas, les collectivités publiques du canton ne disposaient pas encore d'une messagerie électronique instantanée et aucun guichet virtuel permettant d'accomplir des démarches administratives en ligne 24 h/24, 7 j/7 n'était à disposition du public.
2. Avec le recul, on peut dire que la LPrD a permis d'atteindre un niveau de protection appréciable dans les domaines où les défis étaient déjà connus au moment de son entrée en vigueur et qu'elle a montré une étonnante capacité d'adaptation face aux changements rapides auxquels elle a été confrontée. Mais, à l'instar des autres lois sur la protection des données ayant été adoptées au début des années 1990, les dispositions qu'elle contient sont aujourd'hui en partie dépassées par les développements techniques et sociétaux survenus au cours des 30 dernières années. C'est pourquoi elles nécessitent d'être modernisées et complétées.
3. Cette volonté de modernisation n'est pas propre au canton de Fribourg. Elle s'inscrit dans un mouvement général en Europe et en Suisse tendant, d'une part, à renforcer les droits et les libertés des personnes concernées face aux traitements toujours plus nombreux et complexes de leurs données personnelles et, d'autre part, à améliorer la sécurité des infrastructures, des processus et de l'organisation qui soutiennent ces traitements. La nouvelle loi fédérale sur la protection des données a été adoptée le 25 septembre 2020 et entre en vigueur le 1er septembre 2023. Du côté des cantons, la moitié a d'ores et déjà procédé à la révision de leur propre loi et l'autre moitié est en train de le faire.
4. Le projet proposé vise à mettre en conformité le droit cantonal fribourgeois avec les nouveaux standards en matière de protection des données. Il est fortement inspiré par la nouvelle loi fédérale sur la protection des données, laquelle a elle-même pour objectif de rendre le droit fédéral compatible avec la Convention STE 108+ du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et avec les nouvelles exigences du droit de l'Union européenne en matière de protection des données.
5. Quand bien même la nouvelle loi fédérale sur la protection des données a exercé une influence importante sur la réalisation du présent projet, celui-ci n'en constitue pas pour autant une simple copie. Il tient compte notamment de particularités propres au canton de Fribourg et aussi des expériences menées par le canton en matière de digitalisation. On peut citer à titre d'exemple les éléments suivants :
   - les règles introduites en 2020 par la loi adaptant la législation cantonale à certains aspects de la digitalisation au sujet de l'externalisation du traitement de données ont fait leur preuve et ont été reprises quasiment à l'identique dans le projet ;
   - pour respecter la composition bipartite de l'Autorité cantonale de la transparence, de la protection des données et de la médiation, les nouveaux pouvoirs qui sont accordés à l'Autorité ne sont pas concentrés dans les seules mains du ou de la préposé-e mais ont été répartis entre celui-ci/celle-ci et la Commission cantonale de la transparence, de la protection des données et de la médiation ;
   - contrairement à la nouvelle loi fédérale sur la protection des données, le projet ne prévoit pas de supprimer la protection des données des personnes morales pour des raisons à la fois juridiques et de praticabilité.
6. Néanmoins, il faut préciser que le projet s'inscrit dans un cadre relativement strict qui ne laisse pas beaucoup de marge de manœuvre. En plus d'offrir une meilleure protection, les nouveaux droits en faveur des personnes dont les données sont traitées et les nouvelles obligations auxquelles seront désormais astreints les responsables du traitement visent de manière générale à aligner la législation fribourgeoise en matière de protection des données sur les nouveaux standards applicables dans ce domaine à l'ère de la digitalisation. La mise en œuvre de ces

standards est aussi une condition nécessaire de la réussite et du succès du passage à la cyberadministration dans la mesure où il ne peut y avoir de digitalisation sans confiance numérique.

# 1 Généralités

—

## 1.1 Contexte et origine du projet

**1.1.1.** En matière de protection des données, plusieurs générations de législations se sont succédé afin d'encadrer les nouvelles pratiques et définir les garde-fous nécessaires aux traitements de données personnelles face aux développements constants des outils numériques :

a) La première génération de ces législations s'étend des années 1980 à 2000. Inspirée principalement par l'ancienne Convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE 108 ; RSF 0.235.1), elle est caractérisée par une approche fondée sur des grands principes (licéité, proportionnalité, finalité, bonne foi, exactitude *etc.*) qui doivent servir à encadrer des pratiques et des risques encore mal connus. Dans l'Union européenne, le premier texte de référence en la matière est l'ancienne Directive 95/46/CE sur la protection des données promulguée en 1995. En Suisse, la Confédération adopte en 1992 la loi fédérale sur la protection des données (LPD ; RS 235.1). Certains cantons l'avaient précédée à l'image du canton de Berne dont la loi sur la protection des données (LCPD ; RSB 152.04) remonte à 1986 ; les autres lui emboîtent le pas dans les années qui suivent, à l'instar du canton de Fribourg dont la LPrD date de 1994.

b) La deuxième génération se développe peu à peu à partir des années 2000 et s'étend sur une période d'environ quinze ans durant lesquelles le numérique va connaître un essor sans précédent. Le droit de la protection des données commence à se matérialiser sous l'effet conjugué des apports de la doctrine et des décisions de justice qui se succèdent. Les grands principes sont complétés par des règles plus précises. La Convention STE 108 évolue : un Protocole additionnel est adopté en 2001 qui impose de nouvelles obligations aux Etat membres, notamment celle de renforcer les pouvoirs de leurs autorités de protection des données. Durant cette période, la Confédération adhère aux Accords de Schengen et de Dublin et s'engage dans ce contexte à respecter la Décision-cadre 2008/977/JAI. Elle procède également à deux révisions de la LPD : la première, qui date de 2007, avait pour but de moderniser le contenu de la loi sur quelques points ; la deuxième, qui remonte à 2010, visait à adapter le droit fédéral aux nouvelles exigences de la Convention STE 108, en particulier son Protocole additionnel, et à celles du droit de l'UE. A l'échelon cantonal, les changements apportés sont variables. Certains cantons, à l'instar de Fribourg, se limitent à reprendre le droit supérieur. Mais d'autres cantons vont plus loin et procèdent à des améliorations plus substantielles de leur législation.

c) La troisième génération débute avec l'adoption en 2016 du Règlement général sur la protection des données de l'Union européenne (RGPD) et de la Directive sur la protection des données en matière de poursuite pénale ; cette première série de textes se poursuit en 2018 avec la promulgation de la nouvelle Convention STE 108 révisée (Convention STE 108+). Sans faire table rase des anciennes règles qui ont fait leur preuve, cette dernière génération aborde la question de la protection des données de manière plus large et dynamique que les précédentes en y intégrant la technique et l'organisation. On y trouve en particulier des indications sur la façon dont les systèmes d'information doivent être conçus avec l'introduction des principes de la protection des données dès la conception (*privacy-by-design*) et par défaut (*privacy-by-default*), ainsi que l'instauration de nouveaux droits en faveur des personnes concernées comme le droit à l'oubli et le droit à la portabilité des données. C'est dans ce contexte que la Confédération adopte le 25 septembre 2020 la nouvelle loi révisée sur la protection des données (FF 2020 7397) qui entre en vigueur le 1er septembre 2023. Elle est suivie par l'ensemble des cantons qui procèdent à leur tour à la révision de leur propre loi sur la protection des données.

**1.1.2.** Adoptée en 1994, la loi fribourgeoise sur la protection des données (LPrD ; RSF 17.1) a connu à ce jour deux révisions d'une certaine importance :

La première, par la loi du 8 mai 2008 sur la protection des données (adaptation au droit international, en particulier aux accords Schengen/Dublin ; ROF 2008_053). A l'origine, le projet de révision comptait trois volets (Message du 4 mars 2008, in : BGC 2008 657) :

> adaptation de la loi cantonale aux accords de Schengen/Dublin et au Protocole additionnel du 8 novembre 2001 à la Convention STE 108 ;
> adaptations aux autres corrections apportées dans la loi fédérale sur la protection des données ;
> prise en compte des expériences faites avec la LPrD depuis son entrée en vigueur.

Mais, au final, la révision s'est limitée au premier volet. Selon le Message d'alors du Conseil d'Etat, « il est [...] apparu qu'il ne serait pas possible de réaliser les trois volets de cette révision dans les délais impartis par la Confédération pour l'adaptation des lois cantonales aux accords Schengen/Dublin. Le mandat du groupe de travail a par conséquent été limité au premier volet, à savoir l'adaptation de la LPrD aux exigences du droit international. Les deux autres volets d'adaptations seront réalisés ultérieurement ».

La seconde, en 2020, dans le cadre de la loi du 18 décembre 2020 adaptant la législation cantonale à certains aspects de la digitalisation (ROF 2020_195). Même si cette seconde révision avait déjà pour objectif d'adapter le cadre légal à certaines pratiques nouvelles, elle était néanmoins concentrée sur la question spécifique du recours au *cloud computing*. Son objectif n'était pas de procéder à une révision de la LPrD pour la mettre en conformité avec les nouvelles exigences apparues dans ce domaine.

**1.1.3.** Autrement dit, la LPrD se situe aujourd'hui globalement à mi-chemin entre la première et la deuxième génération des législations sur la protection des données. C'est pourquoi l'exercice consistant à procéder à sa révision totale semble difficilement évitable à ce stade. Il doit servir à doter le canton de Fribourg d'un cadre juridique moderne qui non seulement offre aux citoyens et aux citoyennes une protection adaptée et cohérente en matière de protection des données, mais qui répond aussi aux exigences et aux standards du droit fédéral, du droit européen et de la Convention STE 108+ du Conseil de l'Europe (sur les aspects de droit international, voir § 1.3.2).

## 1.2 Déroulement des travaux

**1.2.1.** A la fin de l'été 2017, le Conseil fédéral a adopté son projet de révision totale de la LPD. Dans la foulée, la Chancellerie d'Etat a demandé à l'Autorité cantonale de la transparence et de la protection des données (ATPrD ; aujourd'hui Autorité cantonale de la transparence, de la protection des données et de la médiation, ATPrDM) de constituer un groupe de travail afin de procéder à l'analyse des dispositions de la législation fribourgeoise sur la protection des données et de proposer les adaptations qui s'imposent à la lumière des modifications de la LPD proposées par le Conseil fédéral et des nouvelles normes de droit international qui ont un impact sur la Suisse dans ce domaine.

**1.2.2.** Le groupe de travail constitué par l'ancienne préposée à la protection des données comprenait des personnes représentant chacune des Directions, le pouvoir judiciaire, le Ministère public, la Police, le Service de l'informatique et des télécommunications (ci-après : SITel), les communes ainsi que le Service de législation (ci-après : SLeg). Il a remis un avant-projet d'acte qui a fait l'objet d'une consultation à la fin de l'année 2019.

**1.2.3.** Les retours de la consultation ont montré que, sur le fond, personne ne conteste la nécessité de réviser la LPrD dans sa globalité. Toutefois, plusieurs organes des collectivités publiques redoutent une surcharge de travail liée à la mise en œuvre de la nouvelle loi et réclament pour ce faire l'octroi de ressources supplémentaires. Certains ont relevé le caractère compliqué du projet et ont demandé que celui-ci soit simplifié, tandis que d'autres, à l'inverse, ont dénoncé l'usage de nombreux principes généraux formulés de manière vague et ont demandé plus de précisions sur ce qui était concrètement attendu. De nombreuses remarques ciblées ont été formées par rapport à des dispositions spécifiques.

**1.2.4.** Suite à la consultation, le projet a volontairement été mis en *stand-by* le temps de connaître le texte définitif de la loi fédérale. L'apparition de la pandémie de COVID-19 a prolongé ce statut dans la mesure où elle a exigé de nombreuses ressources juridiques pendant la période 2020-2021. Ce n'est qu'à la fin de l'année 2021 que le groupe de travail chargé de la révision de la LPrD a été reconstitué sous une forme plus restreinte réunissant des représentants et des représentantes des Directions (DFIN, DAEC et DSJS), de l'ATPrDM, du SITel et des communes. Le groupe de travail a par ailleurs été placé sous la responsabilité d'un membre du SLeg. Le nouveau groupe de travail a terminé ses travaux en septembre 2022.

**1.2.5.** Lors des travaux de mise au point du texte, le groupe de travail a le plus possible tenu compte des remarques ciblées émises lors de la consultation de 2019 et a tenté d'y donner suite lorsque c'était possible et opportun. En revanche, il n'a pu que constater, sans réelle possibilité d'action, que la mise en œuvre des nouveaux standards en matière de protection des données allait logiquement exiger des efforts mais aussi des ressources supplémentaires. Afin de répondre aux critiques sur le caractère compliqué de l'acte, le groupe de travail a procédé à plusieurs adaptations visant à retirer ce qui paraissait inutile et non indispensable et à simplifier certaines formulations. Il n'en résulte pas forcément un texte plus court, mais un texte plus lisible et facile à manipuler en dépit d'une matière qui, elle, reste forcément complexe.

**1.2.6.** En septembre 2022, l'ancienne préposé-e à la protection des données a quitté ses fonctions. L'ATPrDM a alors annoncé qu'elle désirait saisir cette occasion pour expérimenter un nouveau mode d'organisation réunissant auprès d'une seule et même personne les deux fonctions de préposé-e à la transparence et de préposé-e à la protection des données. A cette fin, le Conseil d'Etat a nommé la préposée à la transparence préposée à la protection des données *ad interim* et a octroyé un délai pour tester cette nouvelle configuration. La Chancellerie d'Etat en a profité pour organiser dans l'intervalle une nouvelle consultation interne sur le texte remanié. Cette deuxième consultation interne s'est déroulée du 25 octobre 2022 au 27 janvier 2023.

**1.2.7.** Les résultats de la deuxième consultation ont globalement révélé des résultats assez semblables à ceux de la première consultation de 2019. Même si les critiques contre le nouveau texte se sont globalement estompées, les organes de l'administration continuent de craindre une surcharge de travail et réclament de nouvelles ressources. Certaines remarques ciblées ont conduit à apporter d'ultimes précisions ou corrections soit dans le texte de l'acte, soit dans le Message qui l'accompagne.

**1.2.8.** Il convient encore de noter que l'ATPrDM a participé à toutes les phases du projet. Cette participation appréciée et constructive a permis au projet d'évoluer dans de bonnes conditions et d'apporter les meilleures solutions possibles là où c'était nécessaire. Le projet reçoit ainsi un écho favorable de la part de l'Autorité.

## 1.3 Grandes lignes du-projet

### 1.3.1 Contenu en général

**1.3.1.1.** Le contenu des dispositions proposées s'inspire en grande partie de la nouvelle loi fédérale, laquelle est elle-même fortement inspirée par la Convention STE 108+, le RGPD et la Directive (UE) 680/2016. Ces réglementations ont influencé le contenu du projet principalement à trois niveaux :

a) Le projet reprend l'approche fondée sur les risques qui caractérise les nouvelles législations sur la protection des données. Selon cette approche, les obligations en matière de protection des données sont plus strictes pour les responsables de traitement dont les activités présentent un risque accru d'atteinte aux droits fondamentaux que pour ceux dont les activités sont moins risquées (cf. FF 2017 6565, p. 6593). Cela est notamment illustré à l'article 11 du projet.

b) Le projet conserve aussi le caractère technologiquement neutre des règles proposées. Ceci ne l'empêche pas pour autant de réglementer certaines pratiques plus récentes qui sont étroitement liées à l'utilisation des nouvelles technologies comme c'est le cas, en particulier, de l'externalisation de certains types ou de certaines formes de traitements (art. 18 à 21 du projet). Le caractère technologiquement neutre de la réglementation est certes

important si on veut éviter qu'elle ne devienne rapidement dépassée par les progrès de la technologie, mais il ne doit pas amener non plus à ignorer cette dernière au risque que la loi n'atteigne pas ses objectifs.

c) La terminologie employée dans le projet a finalement été modernisée afin d'être plus en phase avec les évolutions du droit de la protection des données et d'améliorer aussi la compatibilité de la loi avec les nouvelles pratiques et les derniers textes légaux de rang fédéral et international dans ce domaine. La notion statique de « fichier » est remplacée par l'expression plus dynamique d'« activité de traitement ». Les données dites sensibles incluent les « données génétiques » et les « données biométriques ». La notion de « profilage » a été spécialement introduite.

**1.3.1.2.** En comparaison avec le projet du Conseil fédéral, le projet compte cependant une différence importante qui mérite d'être soulignée. Il ne prévoit pas de supprimer la protection des données des personnes morales. Deux raisons expliquent principalement ce choix :

a) Sous l'angle strictement juridique, l'article 12 al. 2 de la Constitution fribourgeoise prévoit que toute personne a le droit d'être protégée contre l'usage abusif des données qui la concernent. La norme est semblable à l'article 13 al. 2 de la Constitution fédérale. Or les auteurs en droit public reconnaissent à ce jour, semble-t-il de manière unanime, que le droit constitutionnel à la protection des données vaut tant pour les personnes physiques que pour les personnes morales[1]. Cette position semble également partagée par le Tribunal fédéral dans plusieurs arrêts récents[2]. De ce point de vue, il peut paraître problématique de se servir d'une révision de la loi pour restreindre le champ d'application d'une norme de rang constitutionnel.

b) Sous l'angle pratique, le fait de supprimer la protection des données des personnes morales aurait pour conséquence, selon le Conseil fédéral, que les bases légales qui habilitent aujourd'hui les organes publics à traiter des données personnelles deviendraient caduques s'agissant des données de personnes morales (Cf. FF 2017 6565, p. 6595 et 6603 s et 6633). Pour le Conseil fédéral, cette situation est problématique sous l'angle du principe de la légalité en vertu duquel toute activité de l'Etat doit être fondée sur la loi (Cf. FF 2017 6565, p. 6722 et 6733). Afin de permettre aux organes publics de continuer de traiter les données de personnes morales, il a jugé nécessaire de réintroduire toute une série de dispositions dans la LOGA qui reprennent, au bout du compte, sous une forme très proche le contenu des dispositions de la LPD mais pour les personnes morales (cf. les articles 57h$^{bis}$, 57i, 57j, 57k, 57l, 57r, 57s, 57t LOGA tels qu'introduits par la n-LPD). Il a procédé au même exercice avec la législation spéciale où les règles qui autorisent le traitement des données personnelles ont été doublées pour autoriser aussi le traitement des données de personnes morales (p. ex. : art. 9 LTrans ; art. 15b LSR ; art. 5, 14a, 15 et 19 LSF ; art. 17a LTN, tels qu'introduits par la n-LPD). Dans ce contexte, il semble que la suppression des données des personnes morales s'apparente, dans le domaine du droit public en tout cas, plus à un exercice de style qu'à un véritable changement de pratique. C'est pourquoi, elle n'a pas été reprise dans le projet fribourgeois. D'autres cantons, à l'instar des cantons de Genève ou de Zurich, ont fait la même analyse et ont renoncé à supprimer la protection des personnes morales dans leur propre loi sur la protection des données.

### 1.3.2 Liens avec le droit de l'Union européenne et la Convention STE 108 modernisée

**1.3.2.1.** Plusieurs textes de droit international ont influencé le présent projet à des degrés divers. Il s'agit du RGPD, de la Directive (UE) 2016/680 sur la protection des données dans le domaine de la police et de la justice et de la Convention STE 108+.

**1.3.2.2.** Parmi ces textes, seule la Directive (UE) 2016/680 présente à ce jour une portée obligatoire pour la Suisse, car elle constitue un développement de l'acquis de Schengen (FF 2017 6565, p. 6587 et 6613 ss). Son champ d'application est toutefois limité à certains domaines tels que la justice, la police ou l'asile. La Directive (UE)

—

[1] DUBEY Jacques, *Droits fondamentaux, vol. II*, Bâle 2018, n° 1766 ; BIAGGINI / GIOVANNI, *BV Kommentar*, Zurich, 2e éd., 2017, ad art. 13, n° 12 ; SCHWEIZER Rainer J., in Ehrenzeller Bernhard *et alii* (édit.), *St.Galler Kommentar der Schweizerische Bundesverfassung*, 3e éd., Zurich / Bâle / Genève 2014, ad art. 13, n° 73 ; MALINVERNI / HOTTELIER, HERTIG RANDALL / FLÜCKIGER, *Droit constitutionnel suisse, vol. II*, 4e éd., Berne 2021, n° 408 ; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, 4e éd., Berne 2008, p. 166 ; DIGGELMAN Oliver, in Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (édit.), Basler Kommentar Bundesverfassung, Bâle 2015, *ad* art. 13, n° 33.

[2] ATF 144 II 77, consid. 5 ; ATF 144 II 91, consid. 4.4.

2016/680 n'étant pas directement applicable ni pour les Etats membres de l'Union européenne, ni pour la Suisse, elle doit être transposée en droit interne. Cela implique pour le canton de Fribourg d'adapter non seulement son droit de la protection des données mais aussi certaines autres lois cantonales qui entrent dans le champ d'application de la Directive.

**1.3.2.3.** Selon le Conseil fédéral, la Suisse n'est en revanche pas directement liée par le contenu du RGPD (cf. FF 2017 6565, p. 6587 et 6613 ss). Il n'empêche toutefois que celui-ci exerce une influence indirecte non-négligeable. Car l'échange sans condition de données entre des responsables du traitement européens et suisses est soumis à la condition que l'Union européenne rende une décision d'adéquation attestant que la législation suisse en matière de protection des données offre un niveau de protection équivalent à la législation européenne (cf. art. 45 RGPD). En l'absence d'une telle décision, chaque échange de données entre l'Europe et la Suisse serait conditionné à l'application de garanties supplémentaires qui devraient à chaque fois être négociées avec le responsable du traitement européen. Pour un pays comme le nôtre qui se trouve au cœur de l'Europe, cette situation serait très difficile tant pour le secteur public que pour les entreprises du secteur privé. Actuellement, la Suisse est au bénéfice d'une décision d'adéquation datant du 26 juillet 2000 (cf. FF 2017 6565, p. 6588). L'Union européenne procède en ce moment à une nouvelle évaluation du droit suisse afin de vérifier sa compatibilité avec le RGPD. Dans le cadre de cette évaluation, elle examine le droit fédéral mais aussi certains droits cantonaux de manière aléatoire. Il est donc essentiel que le canton de Fribourg, à l'instar des autres cantons suisses, adapte sa législation en matière de protection des données.

**1.3.2.4.** La Convention STE 108 du Conseil de l'Europe représente le premier texte de droit international en matière de protection des données. Conclue à Strasbourg le 28 janvier 1981, elle a été ratifiée par la Suisse le 2 octobre 1997, avec une entrée en vigueur le 1er février 1998. En 2018, la Convention STE 108 a été entièrement modernisée dans le but de mieux répondre aux défis que représentent la globalisation, les évolutions technologiques et l'augmentation des flux transfrontières de données pour la protection de la sphère privée et les droits fondamentaux des personnes concernées. Même si elle est moins détaillée et moins dense que le RGPD et que la Directive (UE) 2016/680, la Convention STE 108+ a un contenu très semblable à ces deux textes. L'Assemblée fédérale a adopté le 19 juin 2020 l'arrêté fédéral autorisant le Conseil fédéral à ratifier la version révisée de la Convention STE 108 (FF 2020 5559). Le processus de ratification est cependant toujours en suspens. Jusqu'à l'entrée en vigueur du nouveau texte, la Convention STE 108 de 1981 reste applicable.

### 1.3.3 Droits des personnes concernées

**1.3.3.1.** La question des droits des personnes concernées est traitée à la section 3 du projet. L'un des buts de la révision est de renforcer le contrôle et la maîtrise des personnes concernées sur les informations qu'elles partagent avec les collectivités publiques. Le projet introduit dans ce but de nouveaux droits mieux adaptés aux évolutions des usages numériques et facilite les conditions et les modalités de leur exercice.

**1.3.3.2.** Les nouveaux droits introduits sont notamment les suivants :

a) La possibilité pour toute personne de s'opposer préventivement à la communication de données déterminées la concernant à des tiers (droit de blocage ou d'opposition). A l'heure actuelle, pareil droit est prévu dans le canton de Fribourg uniquement en lien avec les données du contrôle des habitants (cf. art. 18 LCH). Or le droit d'opposition appartient aux droits de défense traditionnels en matière de protection des données sans égard au type de traitement en cause. C'est pourquoi il est introduit à l'article 31 du projet. Le droit d'opposition n'est toutefois pas absolu. Il ne peut pas être invoqué contre une communication de données qui est prévue par la loi et il peut être mis en échec lorsqu'il existe un intérêt public ou privé prépondérant à la communication des données visées.

b) L'introduction d'un nouveau droit à la limitation du traitement qui permet à la personne concernée de geler temporairement certaines utilisations de certaines de ses données tout en permettant au responsable du traitement de continuer de les conserver (art. 33 al. 2 let. b). Le droit à la limitation du traitement constitue une alternative moins radicale au droit à la suppression et à la rectification des données. Il pourra être utilisé notamment dans le

cas où la personne concernée conteste l'exactitude de ses données, la façon dont elles sont traitées ou bien demande leur suppression, lorsque des vérifications sont nécessaires pour vérifier le bien-fondé d'une telle demande.

c) Des moyens de défense spécifiques et adaptés sont introduits dans le CPJA concernant le traitement automatisé des données dans le cadre de procédures. Le premier cas envisagé à l'article 66a CPJA est celui où des algorithmes sont utilisés en soutien à la prise d'une décision soit pour établir des faits, soit pour appuyer un raisonnement en droit. L'autorité qui rend la décision devra expressément en faire mention dans celle-ci et la personne concernée pourra demander, le cas échéant, à connaître la logique et les critères des algorithmes utilisés. Le second cas envisagé est celui où une décision est prise exclusivement sur la base d'un traitement automatisé de données. Cette disposition qui figurait déjà dans l'avant-projet a néanmoins été déplacée à l'article 4a de l'annexe au CPJA sur le traitement électronique des données. Les raisons de ce changement sont expliquées dans le commentaire de l'article concerné.

d) Par rapport à l'avant-projet, le projet introduit, en plus, le principe d'un droit à la portabilité des données mais sans en faire un droit subjectif (art. 32). En raison des conditions techniques particulières qui sont requises pour la mise en œuvre d'un tel droit, il reviendra à la législation spéciale de le prévoir ou directement aux responsables du traitement de le concrétiser dans les infrastructures et/ou les applications qu'ils gèrent.

**1.3.3.3.** Pour le reste, les changements apportés constituent des améliorations et des adaptations ponctuelles des normes existantes, visant à préciser le sens et à faciliter la mise en œuvre des droits existants, notamment le droit d'accéder à ses propres données et les différentes actions défensives dont dispose la personne concernée face à un traitement potentiellement illicite de ses données.

### 1.3.4 Obligations des responsables du traitement

**1.3.4.1.** Les obligations du responsable du traitement sont définies à la section 4 du projet. Il fixe les mesures d'organisation et de sécurité encadrant le traitement de données personnelles par les organes publics et les responsabilités y relatives.

**1.3.4.2.** De manière générale, chaque organe qui traite des données à quelque niveau que ce soit est responsable de leur protection (art. 36). Comme c'est le cas déjà actuellement, cette responsabilité est assurée et mise en œuvre de manière transparente et systématique. Sous réserve de quelques exceptions, tout traitement de données doit faire l'objet d'une annonce auprès du registre des activités de traitement (art. 38 et 39). Il est placé sous la responsabilité d'un ou plusieurs organes responsables qui sont tenus d'assurer la protection et la sécurité des données par des mesures concrètes et adaptées aux circonstances (art. 40). Des règles sont prévues pour régler le cas où un responsable du traitement sous-traite tout ou partie d'un traitement auprès d'une entité tierce (art. 37).

**1.3.4.3.** Par rapport à la situation actuelle, les responsables du traitement se voient imposer des nouvelles mesures à mettre en œuvre dans les différentes phases de traitement mais aussi en amont de celles-ci :

a) Les notions de protection des données dès la conception (en anglais : « *privacy by design* ») et par défaut (en anglais : « *privacy by default* ») sont intégrées dans les dispositions en matière de sécurité (art. 40). La première signifie que des mesures techniques et organisationnelles adaptées doivent être discutées et mises en place dès les premières étapes de la conception d'un nouveau traitement de données afin de préserver le plus tôt possible les droits et les libertés des personnes concernées. La deuxième implique que les données personnelles doivent être traitées avec les moyens et selon les modalités qui, par défaut, assurent le niveau le plus élevé de protection.

b) Avant de débuter un nouveau traitement de données qui est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes concernées, le responsable du traitement est tenu d'accomplir préalablement une analyse d'impact relative à la protection des données (art. 41). Le but de cette analyse d'impact est double : d'une part, aider les responsables du traitement à construire des traitements de données respectueux de la vie privée et, d'autre part, démontrer leur conformité à la loi sur la protection des données.

c) En cas de violation de la sécurité des données, le responsable du traitement est tenu de prendre les mesures nécessaires pour remédier à la situation. En fonction de la situation et de la gravité de la violation, il peut être tenu d'informer le ou la préposé-e, voire, si cela est nécessaire, directement la ou les personnes concernées (art. 43 et 44).

d) Chaque Direction sera tenue de nommer pour elle-même et ses unités administratives un correspondant ou une correspondante à la protection des données (art. 45). Cette personne aura pour fonction, d'une part, de sensibiliser le personnel aux questions et aux enjeux de protection des données au sein de la Direction et, d'autre part, de fournir des conseils et une assistance de première ligne dans ce domaine. A l'ère de la cyberadministration et du tout numérique, il est essentiel que les Directions acquièrent un savoir-faire et une certaine autonomie par rapport à cette thématique. Il en résultera aussi un allègement de la charge de travail de l'ATPrDM et une concentration plus marquée sur son rôle de contrôle et de surveillance.

### 1.3.5 Autorité de surveillance en matière de protection des données

**1.3.5.1.** Selon le droit actuel, l'Autorité de surveillance en matière de protection des données ne dispose pas de pouvoir décisionnel dans son domaine de compétence. Elle peut uniquement effectuer des enquêtes et rendre des recommandations à l'attention des organes publics ne respectant pas ou pas complètement leurs obligations en matière de protection des données en les invitant à remédier aux manquements constatés. La recommandation n'a cependant pas de caractère contraignant. Mais si l'organe public refuse d'y donner suite, il doit en informer l'Autorité qui a la possibilité de porter l'affaire en justice (cf. art. 22a LPrD dans sa version actuelle).

**1.3.5.2.** Le projet renforce la position de l'Autorité de surveillance. Il s'agit là d'une obligation contraignante qui résulte directement de l'article 47 par. 2 de la Directive (UE) 2016/680 et de l'article 15 § 2 let. a et d de la Convention STE 108+. A l'instar des autorités de surveillance de la Confédération et des autres cantons, l'ATPrDM doit disposer non seulement de pouvoirs d'investigation mais aussi de pouvoirs d'intervention lui permettant d'ordonner, le cas échéant, que des mesures soient prises en cas de non-respect des prescriptions en matière de protection des données.

**1.3.5.3.** Afin d'éviter toutefois de concentrer un trop gros pouvoir entre les mains d'une seule personne, le projet prévoit de répartir celui-ci entre le ou la préposé-e et la Commission de la transparence, de la protection des données et de la médiation. Le pouvoir de recommandation, tel qu'il existe aujourd'hui dans la loi, est ainsi attribué au ou à la préposé-e. S'il ou elle constate une violation de la protection des données, le ou la préposé-e pourra, comme c'est le cas déjà actuellement, adresser au responsable du traitement une recommandation (art. 57). Cette recommandation devra indiquer clairement les motifs pour lesquelles le traitement querellé n'est, du point de vue du ou de la préposé-e, pas conforme aux exigences en vigueur et quel type de mesures le responsable du traitement devrait prendre pour y remédier. Ce n'est que si le responsable du traitement refuse de donner suite à la recommandation que le ou la préposé-e pourra saisir la Commission afin que cette dernière prononce une décision contraignante (art. 58). Dans ce cas, le responsable du traitement dispose des droits de partie à la procédure. Il a le droit d'être entendu et il peut aussi recourir contre la décision qui lui est adressée (art. 59).

## 1.4 Changements apportés suite à la consultation de 2019

Par rapport au texte mis en consultation, le projet compte quelques modifications de fond. Il faut dire que la ligne tracée par le droit supérieur ne laisse pas aux cantons une marge de manœuvre particulièrement large. Les changements apportés correspondent ainsi à des corrections ponctuelles motivées le plus souvent par le souhait d'un alignement sur le droit fédéral.

Il existe néanmoins quelques changements qui méritent d'être mentionnés spécifiquement :

a) Le principe de la collecte des données directement auprès de la personne concernée a été supprimé, car il ne correspond plus entièrement à la pratique actuelle (cf. commentaire des art. 12 et 13 LPrD).
b) Une nouvelle exception au champ d'application de la loi a été introduite pour les procédures civiles, pénales et de juridiction administrative en cours. L'avant-projet proposait de renoncer à cette exception générale au profit de

deux exceptions ciblées prévoyant dans ce cas la prévalence des règles de procédure et l'incompétence de l'ATPrDM mais le Pouvoir judiciaire et le Tribunal cantonal n'étaient pas favorables à cette solution qu'ils estimaient peu lisible (cf. commentaire de l'article 3).

c) Les règles sur les projets pilotes ont été entièrement repensées (cf. commentaire de l'art. 22 LPrD et commentaire relatif aux articles 35 à 35b LCyb).
d) Le droit de la personne concernée de disposer du sort de ses données après sa mort a été supprimé, car difficilement applicable en pratique (cf. commentaire des art. 27 à 30 LPrD).
e) Le projet fixe les bases concernant l'introduction d'un droit à la portabilité des données mais sans en faire directement un droit justiciable (cf. commentaire de l'art. 32 LPrD).
f) Les règles concernant les décisions individuelles automatisées ont été déplacées de la LPrD au CPJA (cf. commentaire relatif aux adaptations du CPJA).
g) L'obligation de désigner un correspondant ou une correspondante à la protection des données n'incombe plus à chaque responsable du traitement mais aux Directions (cf. commentaire de l'art. 45 LPrD).
h) A la demande de l'ATPrDM, les fonctions de préposé-e à la transparence et de préposé-e à la protection des données ne sont plus séparées mais sont réunies auprès d'une seule et même personne qui occupera la fonction de préposé-e à la transparence et à la protection des données.
i) A l'instar de la Confédération et des autres cantons et conformément aux règles de l'Union européenne, le ou la préposé-e à la transparence et à la protection des données n'est plus engagé-e pour une durée indéterminée mais est nommé-e pour une période de cinq ans, renouvelable (cf. commentaire de l'art. 51 LPrD). En outre, la répartition des tâches entre le ou la préposé-e et la Commission de la transparence, de la protection des données et de la médiation a été revue et clarifiée (commentaire des art. 48 ss).

## 1.5 Conséquences du projet

*a) Changements dans la pratique administrative*

**1.5.1.** Le renforcement des droits des personnes concernées et des obligations à charge des responsables de traitement aura immanquablement un certain impact sur le mode de fonctionner des organes des collectivités publiques. L'impact réel des changements apportés sur le comportement des personnes concernées comme des organes de l'administration est toutefois difficilement prévisible à ce stade. Si l'on en croit les premiers retours de l'entrée en vigueur dans l'Union européenne du RGPD et de la Directive (UE) 2016/680, un véritable bouleversement des pratiques administratives semble néanmoins peu probable.

**1.5.2.** Contrairement à ce qui s'est passé lors l'entrée en vigueur de la LPrD en 1995, les organes des collectivités publiques n'auront pas à revoir en profondeur leur mode de fonctionner pour se conformer aux nouvelles exigences de la protection des données. La plupart d'entre eux étant d'ores et déjà sensibilisés depuis longtemps aux questions de protection des données, les changements apportés ne constituent pour l'essentiel que des ajustements ponctuels venant compléter 30 ans d'acquis dans ce domaine. En outre, conformément à l'approche fondée sur les risques, ce sont surtout les responsables de traitement qui traitent régulièrement de grandes quantités de données qui seront le plus impactés. Or ces derniers ont, par la force des choses, acquis une expertise renforcée dans ce domaine depuis l'entrée en vigueur de la loi en 1995.

*b) Conséquences financières et en personnel*

**1.5.3.** Dans la mesure où le projet procède pour l'essentiel à une adaptation à du droit supérieur qui est de toute manière obligatoire, il entraine peu, de par lui-même, de nouvelles dépenses. Mais il est vrai que, pour se conformer aux nouvelles exigences du projet, les différents organes de l'Etat devront ponctuellement puiser dans leurs ressources disponibles, notamment lorsqu'il s'agira d'accomplir une analyse d'impact relative à la protection des données ou d'assurer le suivi d'un incident de sécurité. Au niveau de l'administration, c'est essentiellement l'obligation pour les Directions de désigner au minimum un correspondant ou une correspondante à la protection des données qui représentera la charge nouvelle la plus claire. La charge de travail supplémentaire se monte à 0,25 EPT par Direction plus la Chancellerie d'Etat, soit 2 EPT au total. Le projet réserve la possibilité pour le Conseil d'Etat de

prévoir, en plus, la nomination d'un correspondant ou d'une correspondante dans des services ou des établissements qui ont des besoins particuliers dans ce domaine. Mais comme il s'agit seulement d'une faculté, elle n'entraine pas de conséquences financières directes tant qu'elle n'a pas été utilisée. L'introduction des correspondants et des correspondantes à la protection des données conduit ainsi à une dépense nouvelle de CHF 345'000.- par année. Il est, par ailleurs, proposé de coupler cette nouvelle tâche à celle de l'accompagnement de la sécurité de l'information, sujet connexe à celui de la protection des données.

**1.5.4.** Sous l'angle de la technique, il est à noter que le canton de Fribourg s'est engagé dans la voie de la digitalisation dans le cadre de sa stratégie Fribourg 4.0. Certaines initiatives ont d'ores et déjà été lancées dans ce contexte afin de maîtriser au mieux la gestion, la centralisation et la standardisation de certaines catégories de données (p. ex. : le projet Référentiel cantonal). La révision de la loi, associée à la mise en œuvre de la stratégie Fribourg 4.0, s'accompagne inévitablement de nouvelles exigences techniques. Mais ces exigences s'inscrivent pleinement dans les objectifs de standardisation et de concentration des paysages informatiques actuellement à l'œuvre, lesquels conduisent à une révision profonde du traitement de l'information au sein de l'Etat. Il est donc normal d'y associer la protection des données, même si ça n'est pas cette dernière qui en est la cause première. Pour répondre de manière efficace aux nouveaux besoins comme aux nouvelles obligations de l'administration, il sera nécessaire dans certains domaines d'automatiser les processus afin d'alléger les traitements manuels. La mise en œuvre de ces processus automatisés exigera des efforts et aussi un temps d'adaptation. Il faudra en effet construire ou paramétrer les environnements nécessaires à l'exécution des demandes. Cela ne pourra se faire qu'en tenant compte des cycles budgétaires internes à l'administration et aussi de la vétusté de certains systèmes qui devront être remplacés. Dans ce contexte, il y a lieu de s'attendre à moyen ou à long terme à des coûts indirectement induits par l'application de la loi, mais qui correspondent aussi et surtout aux coûts liés à une bonne gestion des ressources et des infrastructures électroniques de l'Etat. Chiffrer ces coûts n'est par conséquent ni faisable, ni vraiment pertinent.

**1.5.5.** Le projet introduit de nouvelles tâches pour l'ATPrDM, en particulier pour le ou la préposé-e à la transparence et à la protection des données. Ces nouvelles tâches viennent s'ajouter à une augmentation générale de la charge de travail à laquelle l'Autorité doit déjà faire face depuis plusieurs années dans le cadre de la digitalisation de l'Etat à laquelle elle participe soit directement en prenant part à plusieurs groupes de travail, soit indirectement au travers des conseils qu'elle rend ainsi que dans le cadre des consultations législatives. Or, depuis sa création en 1994, les ressources en personnel de l'ATPrDM consacrées à la protection des données ont peu augmenté. En 2009, l'ATPrDM a obtenu l'octroi de 0.5 EPT pour un poste de juriste et, en 2020, le poste de préposé-e à la protection des données a été augmenté de 0.3 EPT, passant de 0.5 à 0.8 EPT. L'ATPrDM dispose en sus d'une collaboratrice administrative (0,8 EPT) et d'un ou d'une stagiaire juriste à 100%. Cette dotation a été légèrement remaniée durant la phase d'essai où la préposée à la transparence a été nommée simultanément préposée à la protection des données ad interim (cf. § 1.2.6). La préposée travaillant à un taux de 0.8 EPT, il a été possible de convertir les 0.5 EPT de poste de préposé-e restant en 0.5 EPT de poste de juriste permettant ainsi de disposer d'un poste de juriste à 100%. En outre, la Chancellerie prête actuellement à l'Autorité 0.6 EPT de juriste et 1 EPT de juriste stagiaire. Il est certain que le passage à la nouvelle loi engendrera une augmentation des besoins en personnel de l'Autorité, mais cette augmentation est pour l'heure difficile à chiffrer. Dans tous les cas, un nouvel EPT supplémentaire est d'ores et déjà prévu pour la présente législature. Dans la mesure où cette augmentation est une conséquence de la mise en œuvre d'obligations de droit international qui lient la Suisse, il ne s'agit pas d'une dépense nouvelle mais d'une dépense liée ; elle ne compte pas dans le calcul du referendum financier.

**1.5.6.** Au total, on peut estimer les frais nouvellement et directement imputables à la nouvelle loi à la création de 2 nouveaux EPT. Sur une période de cinq ans, il en résulte une dépense d'environ CHF 1'725'000.-. La présente loi n'est ainsi pas soumise au referendum financier facultatif ni au referendum financier obligatoire.

## 1.6 Conformité au droit supérieur et développement durable

**1.6.1.** Le projet actualise les conditions-cadre du droit à la protection des données garanti à l'article 12 al. 2 de la Constitution du canton de Fribourg du 16 mai 2004. Il fait également en sorte de respecter les engagements pris par la Suisse dans le cadre des accords de Schengen et de Dublin avec l'Union européenne et il satisfait aux exigences de la

Convention STE 108+ que la Confédération a d'ores et déjà ratifiée. Le projet a ainsi précisément pour ambition de mettre la législation fribourgeoise en conformité avec le droit supérieur.

**1.6.2.** Le projet a fait l'objet d'une analyse complète selon la méthode Boussole 21 dans le but d'en dresser les forces et les faiblesses dans les trois dimensions du développement durable (économique, environnementale et sociétale). Il est ressorti de cette analyse que le projet aura un impact sociétal largement positif dès lors qu'il fixe un cadre rassurant au traitement des données personnelles par les organes de l'administration. Du point de vue économique aussi les impacts sont globalement positifs. Il est vrai que les exigences liées à la protection des données sont susceptibles à court terme de freiner l'avancement de certains projets. Mais ces efforts qui participent d'une bonne gouvernance seront récompensés à moyen et à long terme, car ils permettent de disposer d'infrastructures et d'applications robustes et durables. De plus, l'harmonisation du droit cantonal avec les lois de la Confédération, des autres cantons et de l'UE facilitera les échanges entre le canton de Fribourg et l'extérieur. Pour que la future loi puisse atteindre ses objectifs, l'analyse a cependant mis en évidence un fort besoin d'accompagnement induit par la densité et la complexité du texte. La création d'un réseau au sein de l'administration de correspondants et de correspondantes à la protection des données ainsi que la mise en place de formations a été jugé comme l'un des éléments clé nécessaire au succès du projet. Cet accompagnement permettra à moyen terme d'identifier les besoins de soutien existant au sein des Directions pour assurer cette mise en œuvre.

# 2 Commentaire des dispositions

—

## 2.1 Section 1, Dispositions générales

### *Art. 1, But*

L'augmentation continue du nombre de traitements de données et le perfectionnement des moyens à disposition dans ce domaine ont entraîné de profondes modifications du régime juridique de plusieurs droits fondamentaux au premier rang desquels figurent la liberté personnelle et la protection de la sphère privée. Mais d'autres droits sont aussi directement visés tels que la liberté d'expression, la liberté d'opinion ou encore la liberté d'association. Le Tribunal fédéral a, dans ce contexte, reconnu l'existence d'un nouveau droit fondamental à l'autodétermination informationnelle, lequel a pour fonction de donner à la personne concernée une plus grande maîtrise sur les informations qui la concernent[3]. C'est pourquoi, à l'instar de la loi actuelle, le projet indique que la loi vise à protéger les *droits fondamentaux* des personnes concernées, sans préciser lesquels.

### *Art. 2, Champ d'application personnel*

1. Le champ d'application personnel du projet est pour l'essentiel calqué sur celui de la loi actuelle. Il recouvre :

    a) L'ensemble des organes qui relèvent des autorités législatives, exécutives et judiciaires aux échelons cantonal, communal et intercommunal, y compris les autres personnes de droit public tels que les établissements de droit public (personnalisés ou non) ou les sociétés de droit public fondées sous la forme d'une société anonyme. Sont également visés des organismes particuliers comme le Conseil de la magistrature.

    b) Certaines personnes privées, physiques ou morales, lorsqu'elles sont chargées de l'accomplissement de tâches publiques. La formule reprend celle utilisée à l'article 2 let. *d* CPJA . La loi leur sera toutefois applicable uniquement pour la partie de leurs activités relevant de la tâche publique en question. Parmi les institutions visées, on peut citer l'Union fribourgeoise du tourisme ou la ligue fribourgeoise contre le cancer concernant l'exploitation du registre cantonal des tumeurs.

—

[3] Notamment : ATF 145 IV 42, consid. 4.2 ; ATF 144 I 126 consid. 4 ; ATF 143 I 253 consid. 4.

2. Comme c'est déjà le cas sous l'empire de la loi actuelle, l'alinéa 2 traite la question des Eglises reconnues. Conformément à la LEE, les paroisses, les corporations ecclésiastiques et les personnes juridiques canoniques sont des personnes morales de droit public. Pour cette raison, elles entrent dans le champ d'application de la législation cantonale en matière de protection des données. Le projet réserve toutefois la possibilité pour les Eglises d'adopter leurs propres dispositions et d'instituer leur propre autorité de surveillance en matière de protection des données. A ces conditions, elles peuvent demander à sortir du champ d'application de la loi cantonale et à s'autogérer.

### *Art. 3, Champ d'application matériel*

1. Le champ d'application matériel de la loi est volontairement le plus vaste possible (cf. al. 1). Certains types de traitement particuliers y échappent cependant. C'est le cas :

   a) *Des traitements de données effectués dans le cadre de procédures civiles, pénales et de juridiction administrative en cours*. Initialement, l'avant-projet prévoyait d'abandonner ce motif d'exception général en faveur de deux exceptions plus ciblées. Durant toute la durée de la procédure, les prétentions prévues par la présente loi auraient été gelées et l'ATPrDM aurait été déclarée incompétente. Cela permettait en particulier de garantir que les règles relatives à la sécurité des données restent applicables. Mais le Pouvoir judiciaire et le Tribunal cantonal n'étaient pas convaincus par cette solution qui s'écarte du standard des autres lois sur la protection des données en Suisse. C'est pourquoi l'exception relative aux procédures juridictionnelles en cours a été réintroduite. Ce motif d'exception concerne uniquement les traitements de données relatifs à une procédure pendante. Les organes judiciaires restent ainsi soumis à la loi sur la protection des données pour les autres traitements qu'ils accomplissent (gestion du personnel, correspondance hors procédure, communication avec le reste de l'administration, etc.) ou une fois la procédure terminée. En droit administratif, l'exception ne s'applique pas aux procédures administratives de première instance qui restent intégralement soumises à la loi sur la protection des données. Seules les procédures devant les autorités de la juridiction administrative au sens de l'article 3 CPJA tombent ainsi sous le coup de ce motif d'exception.

   b) *Des traitements de données qui servent à l'usage exclusivement personnel de celui ou celle qui les effectue.* Ce motif d'exception ne figurait pas dans l'avant-projet. Il concerne les traitements de données accomplis par une personne au service de l'Etat pour son usage exclusivement personnel. L'introduction de cette exception, qu'on retrouve à l'article 2 al. 2 let. a n-LPD comme dans d'autres lois cantonales, a expressément été demandée dans le cadre de la consultation. Elle présente toutefois une portée limitée. Elle ne peut plus être invoquée sitôt que les données en question sont utilisées de manière officielle, qu'elles sont partagées avec une tierce personne ou qu'elles sont simplement mises à disposition sur un serveur partagé. Concrètement, cette exception se limite aux réflexions individuelles qu'un individu mène pour forger sa propre opinion dans une affaire et qu'il ou elle ne partage pas.

   c) *Les traitements de données accomplis par un organe public en situation de concurrence économique avec des personnes de droit privé.* Pareille exception est nécessaire pour ne pas créer de distorsion en matière de concurrence. Les traitements de données concernés sont soumis à la partie de la loi fédérale sur la protection des données réservée aux personnes privées. Le champ d'application de cette exception est toutefois limité. Seuls peuvent s'en prévaloir les organes publics qui mènent des activités en situation de concurrence économique et pour *autant* qu'ils n'agissent pas en qualité d'organes investis de la puissance publique. C'est le cas, en principe, de la Banque cantonale, sauf dans les activités où elle dispose d'un monopole de droit public (p. ex. : art. 7 al. 1 LBCF). Contrairement à l'avant-projet, le projet renonce à confier la surveillance de ce type de traitements à l'ATPrDM comme c'est le cas, notamment, dans le canton de Berne (cf. art. 4 al. 2 let. a, 2$^{e}$ phr. LCPD/BE). D'une part, le Préposé fédéral à la protection des données a fait valoir lors de la consultation qu'il n'était pas favorable à cette solution, car il estime qu'elle empiète sur ses propres compétences. D'autre part, vu les ressources limitées dont dispose l'Autorité, il est préférable que celle-ci se concentre sur ses tâches primaires.

2. Par rapport à la situation actuelle, l'exception fixe concernant les délibérations du Grand Conseil, des assemblées communales ou des conseils généraux, des assemblées bourgeoisiales ainsi que de leurs commissions (art. 2 al. 2 let. a LPrD) tombe. Cette exception était motivée autrefois par le principe du secret qui prévalait à l'intérieur de l'Etat et la volonté en découlant de bloquer la possibilité pour une personne d'exercer son droit d'accès à ses propres données lorsqu'elles étaient traitées par ce type d'organes. Or ce principe a depuis largement été battu en brèche notamment avec l'adoption en 2009 de la LInf, qui a introduit le principe de la transparence. De plus, cette règle fait l'objet en doctrine de plusieurs critiques[4] et ne subsiste en Suisse que dans une minorité de cantons (GE ; VD ; NW et BE). Sa suppression semble de ce fait parfaitement viable pour les organes visés. Du reste, elle n'a donné lieu à aucune contestation dans le cadre de la consultation. Concernant l'application dans ce domaine du droit d'accès à ses propres données et des autres droits connexes, il sera toujours possible, dans des cas justifiés, de restreindre ou de refuser leur exercice mais uniquement de manière motivée et sur la base d'une pesée d'intérêts dûment réalisée.

### *Art. 4, Définitions*

La quasi-totalité des définitions contenues dans cet article sont reprises textuellement ou presque de la n-LPD au niveau fédéral. On peut donc se référer globalement aux explications données à ce sujet dans le Message du Conseil fédéral (cf. FF 2017 6565, p. 6639 ss.) et se contenter ici des précisions suivantes :

> La notion de procédure d'appel qu'on retrouve à l'article 14 al. 4 du projet est introduite dans les définitions (let. e). Cette forme particulière de communication de données était jusqu'ici décrite uniquement dans un acte du Conseil d'Etat. Vu son importance, il a été jugé opportun d'insérer cette définition à l'échelon de la loi.

> A l'instar de la nouvelle loi fédérale (art. 5 let. f LPD) et du droit de l'UE (art. 3 par. 4 de la Directive (UE) 2016/680 et art. 4 par. 4 RGPD), le projet introduit la notion de profilage (let. f). Il s'agit d'un nouveau type de traitement automatisé de données considéré comme particulièrement intrusif. Il consiste à mettre volontairement en évidence ou à prédire certaines caractéristiques personnelles essentielles d'une personne, notamment dans le but de lui appliquer un traitement particulier. C'est pourquoi le profilage est soumis aux mêmes conditions que le traitement de données sensibles.

> Conformément aux modifications introduites lors de l'adoption de la loi du 18 décembre 2020 adaptant la législation cantonale à certains aspects de la digitalisation (RO 2020_195), le projet inclut une définition de l'externalisation du traitement de données (let. g). Cette définition vient en soutien des articles 18 à 21 qui énoncent les conditions auxquelles une externalisation est permise. Par rapport à la définition introduite en 2021, la nouvelle définition a toutefois été précisée sur deux points. Premièrement, elle indique que l'externalisation est une forme de sous-traitance qualifiée. Ceci justifie qu'elle soit soumise à des règles spéciales. Deuxièmement, pour permettre de bien différencier l'externalisation de la sous-traitance, le projet précise en toutes lettres que l'externalisation concerne ici le recours à des outils d'informatique en nuage (*cloud computing*).

> A l'instar de la n-LPD et de la Convention STE 108+, le projet abandonne la notion de « *fichier* » devenue désuète au regard du caractère ubiquitaire des données. Celle-ci est remplacée de manière générale par l'expression plus large et dynamique d'« *activité de traitement* ». De ce fait, le « responsable du fichier » mentionné à l'art. 4 al. 1 let. g de la loi actuelle devient le « responsable du traitement » (let. h) et le registre des fichiers qu'on trouve actuellement à l'article 21 LPrD est renommé dans le projet « registre des activités de traitement » (let. j et art. 38 du projet). Globalement, ces changements restent néanmoins avant tout d'ordre terminologique et ne devraient pas avoir d'incidences pratiques importantes.

[4] MAURER-LAMBROU Urs / KUNZ Simon, op. cit., n° 23. Egalement : ZUFFEREY Jean-Baptiste, *Les règles de la procédure administrative face à la protection des données – Combat ou complémentarité ?*, in RFJ, numéro spécial : « Le droit en mouvement », 2002 169, p. 176.

> Vu son rôle central dans la mise en œuvre de la protection des données, il est proposé de donner une définition du « *registre des activités de traitement* » (let. j). Celui-ci constitue à la fois un outil de transparence et de gouvernance. Il implique notamment que le responsable d'un traitement de données soit à même de déterminer, pour chaque traitement, qui traite des données, quelles sont les catégories de personnes concernées, quelles sont les données traitées, dans quel but, selon quelles modalités, qui a accès à ces données, combien de temps elles sont conservées, quelles mesures de sécurité ont été prises etc.

> Contrairement à l'avant-projet, le projet introduit la définition de ce qu'est une « *violation de la sécurité des données* » (let. k) et s'aligne ainsi sur l'article 5 let. h n-LPD et sur le droit de l'UE (art. 3 ch. 12 de la Directive (UE) 2016/680 et art. 4 ch. 11 RGPD). Cette définition vient en appui des articles 43 et 44 qui indiquent les mesures à prendre si un tel évènement se produit.

Par rapport à l'avant-projet, le projet renonce à définir les identifiants de personnes et, par voie de conséquence, à réglementer cette thématique dans la loi. Depuis la libéralisation du numéro AVS prévue par le droit fédéral et la création de l'identificateur cantonal de personne (ICP) prévu dans la LCyb, la nécessité de légiférer sur ce thème n'est plus avérée.

## 2.2 Section 2, Principes régissant le traitement de données personnelles

### 2.2.1 Section 2.1 : Conditions générales de licéité du traitement

#### *Art. 5, Base légale*

1. Le traitement de données personnelles par des organes publics est une activité étatique soumise au principe de la légalité (al. 1). La question de savoir quel degré de précision doit avoir la disposition légale et à quel niveau elle doit se situer dépend de l'importance des risques d'atteintes aux droits des personnes que représente le traitement prévu.
2. S'alignant sur la pratique de la Confédération et des autres cantons, le projet pose des exigences plus sévères sous l'angle de la légalité à l'égard des traitements de données personnelles qui présentent des risques accrus pour les droits des personnes (données sensibles, profilage, création de risques particuliers). Ce type de traitements n'est licite généralement que si une base légale au sens formel l'autorise expressément (al. 2 let. a et al. 3). Au niveau des communes, cela correspond à un règlement de portée générale. Pour les traitements de données sensibles, une base légale indirecte peut toutefois être suffisante dans certaines situations, si le traitement est indispensable à l'exécution d'une tâche prévue dans une loi au sens formel et qu'il n'en résulte pas de risques particuliers pour les personnes concernées (al. 2 let. b). Cette règle découle du fait que le législateur ne peut pas toujours prévoir en amont l'ensemble des traitements de données sous-jacents à l'accomplissements d'une certaine tâche.
3. L'Autorité cantonale de surveillance a, jusqu'ici, toujours exigé une base légale au sens formel pour ces types de traitement même en l'absence d'une telle exigence explicite dans la loi. Vu la bonne acceptation de cette pratique au sein de l'administration, ce changement ne devrait pas exercer une influence pratique considérable. Il exigera néanmoins de vérifier que les traitements en cours sont en adéquation avec la règle. Un délai transitoire de deux ans est spécialement prévu à cette fin (cf. art. 63 du projet).
4. S'agissant de la manière de rédiger les bases légales nécessaires au traitement des données, le Service de législation a rédigé un document qui vise à fournir aux juristes de l'administration cantonale un outil et une méthode les aidant dans cette tâche. Ce document est disponible sur la page Internet du Service de législation (https://www.fr.ch/cha/sleg). Dans la mesure où il s'agit d'un document du Service de législation, son contenu ne lie naturellement pas l'ATPrDM. Il constitue simplement une aide à la rédaction.
5. Exceptionnellement, une base légale n'est pas nécessaire lorsqu'un traitement de données, en particulier une communication, est rendue indispensable pour sauvegarder des intérêts essentiels de la personne concernée ou d'un tiers, comme la vie ou l'intégrité corporelle (al. 4). Il s'agit d'une exception dont le champ d'application est

toutefois très étroit et dont l'utilisation en pratique devrait être limitée au domaine des urgences médicales, voire, éventuellement, policières.

### *Art. 6, Consentement*

1. Le consentement de la personne concernée constitue le fait justificatif extra-légal le plus important en droit de la protection des données. Il n'y a, en principe, pas d'atteinte aux droits de la personne concernée lorsque cette dernière accepte que des données personnelles la concernant soient récoltées et traitées à des fins qu'elle a elle-même choisies. En droit public, le consentement ne peut toutefois intervenir généralement que dans un cas d'espèce et ne peut pas remplacer l'adoption d'une base légale (al. 1).
2. L'alinéa 2 fixe les conditions de validité du consentement. Pour être valable, le consentement doit tout d'abord être libre et éclairé. Cela signifie, d'une part, que la personne qui consent doit avoir été dûment informée du but et des modalités du traitement de manière transparente et compréhensible et, d'autre part, que la personne conserve la possibilité de refuser le consentement sans subir de préjudice. Pour les traitements de données sensibles et les activités de profilage le consentement doit être exprès. C'est le cas, en particulier, lorsque la personne concernée accepte une déclaration de consentement en bonne et due forme. On trouve déjà ce type de déclarations pour certaines prestations proposées sur le guichet virtuel. Cela exclut les consentements par actes concluants. Par rapport à l'avant-projet, le projet ajoute que le consentement est présumé lorsque la personne a elle-même rendu ses données librement accessibles. Cet ajout se retrouve en droit fédéral (cf. art. 17 al. 2 let. c LPD / 34 al. 4 let. b n-LPD) et dans presque toutes les lois cantonales. Il concerne, par exemple, les données que la personne concernée a postées sur Linkedin et qui peuvent être traitées par l'autorité d'engagement dans le cadre d'une postulation.
3. Les alinéas 3 à 5 fixent différentes conditions auxquelles les responsables du traitement qui se basent sur le consentement de la personne concernée doivent satisfaire. Le fait de devoir mentionner le caractère facultatif d'un traitement de données qui n'est pas prévu par la loi (al. 3) est une concrétisation du consentement libre et éclairé. La conservation d'un moyen capable de démontrer l'existence du consentement (al. 4) est requise pour des raisons de preuve. Quant à la révocation du consentement (al. 5), elle va de pair avec la faculté de le donner.

### *Art. 7, Finalité*

1. Le principe de finalité est caractéristique du droit de la protection des données. Il se divise en deux volets : *a*) détermination d'une finalité préalable au traitement (principe de détermination du but) et *b*) utilisation des données en fonction de cette finalité ou, du moins, pour une finalité compatible avec celle-ci (principe de compatibilité du but). Ensemble, les principes de détermination et de compatibilité limitent les possibilités d'une ré-utilisation des données en excluant notamment que les données soient collectées de manière illimitée et stockées « en prévision de… ».
2. Le principe de finalité n'est cependant pas immuable. La personne concernée peut valablement consentir à un changement de finalité de ses données si elle y voit un intérêt (al. 2). En principe, une loi peut également déroger au principe de finalité en prévoyant la réutilisation des données à des fins différentes que celles prévues initialement.
3. Par rapport à l'avant-projet, le projet a supprimé l'exigence selon laquelle la finalité prévue doit être légitime. Il est tout à fait possible de parvenir au même résultat sur la base des principes de légalité et de bonne foi comme aussi sur celle de l'interdiction de l'arbitraire.

### *Art. 8, Proportionnalité*

1. Le principe de proportionnalité est un instrument clé de l'ensemble de l'ordre juridique. De façon générale, il postule que les moyens déployés par les pouvoirs publics en vue d'atteindre un certain but ne doivent pas se montrer excessifs et empiéter plus que de raison sur les droits et les libertés des individus.

2. En droit de la protection des données, le principe de proportionnalité signifie que seules les données aptes et nécessaires à atteindre les finalités du traitement peuvent être traitées. Par ailleurs, il doit exister un rapport raisonnable entre les finalités et les moyens utilisés. Les principes d'évitement et de minimisation des données constituent deux expressions du principe de proportionnalité propres au droit de la protection des données. Le premier implique que si le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée. Le second veut que seules les données pertinentes et strictement nécessaires au but poursuivi soient traitées à l'exclusion des autres. En principe, ces deux lignes directrices devraient être respectées dès la conception de nouveaux traitements. Elles sont étroitement liées aux principes de protection des données dès la conception et de protection des données par défaut (cf. art. 40 du projet).

#### *Art. 9, Exactitude*

L'exactitude dont il est question ici est une exactitude relative : en pratique, il est clair que les données qui sont conservées par les différentes collectivités publiques ne peuvent pas être à jour en permanence. Même si elle doit demeurer un objectif plus ou moins constant, l'obligation d'exactitude et de mise à jour des données est avant tout une obligation de moyen et non de résultat. Son étendue dépend des circonstances du cas d'espèce, soit notamment des buts du traitement, de la nature des données traitées et de leur caractère plus ou moins sensible.

#### *Art. 10, Délai de conservation*

1. La conservation des données ne doit pas excéder la durée nécessaire au regard des finalités pour lesquelles elles sont enregistrées. Une fois que l'objectif poursuivi par le traitement des données est atteint, il n'y a, en principe, plus lieu de les conserver et elles doivent être supprimées (ou anonymisées). Cela implique pour les responsables du traitement de vérifier à intervalles réguliers que les données en leur possession sont toujours pertinentes par rapport aux buts visés. Une réserve existe toutefois pour les données qui présentent une valeur archivistique. Ces données ne doivent pas être supprimées mais versées aux Archives[5]. Des précisions supplémentaires à ce sujet figurent aux articles 23 et 24 du projet.
2. Conformément à l'alinéa 2, les données personnelles qui présentent une valeur particulière dans le cadre de recherches, de planifications ou de statistiques n'ont pas besoin d'être supprimées de la même manière, mais peuvent être conservées plus longtemps si des mesures sont prises qui assurent la protection des droits des personnes concernées.

#### *Art. 11, Devoir de diligence accru*

Le devoir de diligence accru qui est demandé face au traitement de données présentant des risques plus importants pour les droits des personnes figure déjà dans le texte de la loi actuelle. Il est une spécialité fribourgeoise qui ne figure dans aucune autre loi en Suisse en matière de protection des données. Même si la règle ne définit pas concrètement quelles sont les mesures à prendre, elle a été maintenue car elle représente une concrétisation de l'approche fondée sur les risques voulant que les plus gros efforts à fournir en matière de protection des données sont à effectuer là où le potentiel de risque est le plus élevé. En pratique, il est question de prendre des mesures techniques et/ou organisationnelles de façon appropriée à la situation et de manière graduelle en fonction du risque.

### 2.2.2 Section 2.2 : Conditions supplémentaires applicables à certaines formes de traitement

#### *Art. 12 et 13, Collecte de données*

1. Comme pour tout traitement, la collecte de données requiert l'existence d'un motif justificatif. Néanmoins, comme cette exigence ressort déjà des articles 5 et 6, le projet renonce à la répéter une deuxième fois ici. C'est la raison pour laquelle l'article 12 al. 1 de l'avant-projet a été supprimé.
2. Par rapport à l'avant-projet, le projet supprime aussi le principe de la collecte des données directement auprès de la personne concernée. Si ce principe était valable au début des années 1990 lorsque la LPrD a été élaborée et qu'il reste aujourd'hui applicable dans plusieurs secteurs d'activité de l'administration, certaines catégories de

[5] Sur la portée de cette réserve : ATF 148 I 233, consid. 4 à 6.

données sont dorénavant collectées une seule fois et ensuite mises à disposition des unités administratives qui en ont besoin pour l'accomplissement de leurs tâches. Cela correspond au principe *Once-Only* que la Confédération et les cantons sont en train de développer. Vu cette évolution, il a semblé inadéquat de conserver ce principe dans la loi.

3. Dans le but d'améliorer la transparence et la reconnaissabilité des traitements, le projet introduit une obligation pour les responsables d'informer les personnes concernées de la collecte de leurs données (art. 12). Cette règle constitue aujourd'hui un standard unanimement reconnu en matière de protection des données, qu'on retrouve en droit fédéral (cf. art. 19 n-LPD) et dans les autres lois cantonales. Les informations à fournir doivent permettre à la personne concernée de comprendre rapidement qui traite des données à son sujet, dans quel but, à qui ses données pourront en principe être communiquées et quels sont ses droits. Les données facultatives qui sont recueillies – par exemple, au moyen d'un questionnaire – doivent être indiquées comme telles. Le débiteur du devoir d'informer est toujours l'organe qui collecte les données et non celui qui les communique. L'organe qui communique les données doit s'assurer que la communication est licite mais n'est pas tenu d'informer la personne concernée de la communication de ses données. Est toutefois réservé l'article 31 al. 3 du projet lorsque la personne a exercé son droit d'opposition.
4. La forme que doit revêtir l'information n'est pas précisée. Le responsable du traitement doit veiller à ce que la personne concernée puisse effectivement prendre connaissance de la collecte des données par un moyen facilement accessible, mais pas à ce qu'elle s'informe effectivement. Un contact direct avec la personne concernée n'est pas exigé. Une information standardisée, par exemple au moyen d'une déclaration de protection des données jointe sur un formulaire ou sur une page Internet, peut être suffisante.
5. Le devoir d'information n'est pas absolu : le responsable du traitement peut être dispensé de son devoir d'information aux différentes conditions mentionnées à l'article 13. Le motif d'exception qui s'appliquera le plus souvent sera alors logiquement l'exécution d'une tâche légale. Dans ce cas, le devoir d'information est réalisé par la publication de la loi. Le devoir d'information peut également être limité ou retardé aux mêmes conditions que celles prévues en matière de droit d'accès à l'article 29 al. 1 (cf. art. 13 al. 2).

### *Art. 14 à 17, Communications de données ordinaires et transfrontières*

1. Une communication de données consiste à rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant, en les diffusant ou en les publiant. Cette notion recouvre aussi bien la communication régulière que la communication dans un cas d'espèce. Les conditions de licéité ne sont cependant pas les mêmes selon que l'on se trouve dans l'un ou l'autre cas :
   a) Conformément à l'article 14 al. 1, les communications systématiques, c'est-à-dire les communications d'un même type de données qui sont adressées aux mêmes destinataires sur une base régulière, doivent être prévues au moyen d'une base légale au sens de l'article 5 du projet ;
   b) En vertu de l'article 14 al. 2, les communications de données qui ont lieu dans un cas d'espèce n'ont pas besoin d'être obligatoirement prévues au moyen d'une disposition légale. Elles peuvent aussi avoir lieu si elles correspondent à l'un des motifs indiqués aux lettres *a* à *c*.
2. Le projet règlemente une troisième catégorie de communication de données : les communications par voie d'appel (art. 14 al. 4). On entend par là un mode d'accès automatisé aux données par lequel le destinataire des données, en vertu d'une autorisation du responsable du traitement, décide de son propre chef, sans contrôle préalable, du moment et de l'étendue de la communication dans les limites de l'autorisation rendue. Au vu des particularités de ce type de communication, il se justifie, pour des raisons à la fois de transparence, de gouvernance et de sécurité, de le mentionner spécifiquement afin de le distinguer des autres formes de communication. Cette exigence n'est pas une nouveauté. Elle est reprise de l'article 10 al. 2 de la loi actuelle.

3. Des exigences supplémentaires s'appliquent en cas de communication de données à l'étranger (art. 15) :

   a) les transferts de données personnelles vers des Etats à l'étranger ne sont en principe autorisés que si l'Etat destinataire offre un niveau de protection des données jugé adéquat. Pour savoir si un Etat offre ou non un niveau de protection adéquat, il est possible de se référer à la liste établie par le Conseil fédéral conformément à l'article 16 al. 1 n-LPD.

   b) Lorsque le pays destinataire est un pays tiers qui n'offre pas un niveau de protection adéquat ou en cas de doute à ce sujet, une communication de données transfrontière reste malgré tout possible en présence d'autres garanties suffisantes ou s'il existe un motif justificatif à la communication (al. 2). Par rapport à l'avant-projet et à la loi actuelle, la liste des garanties suffisantes a été précisée par la mention des mesures techniques et/ou organisationnelles en plus des mesures contractuelles. En pratique, il peut s'avérer nécessaire suivant les cas de cumuler plusieurs types de mesures entre elles.

   Ces règles spéciales ne s'appliquent cependant qu'à la communication de données personnelles se rapportant à des personnes physiques. L'exclusion des personnes morales est nécessaire afin d'assurer que le canton de Fribourg ne se trouve pas soumis à des contraintes supplémentaires dans ses échanges avec l'étranger par rapport aux Etats qui ont sorti du champ d'application de leur loi la protection des données des personnes morales.

   3.1. Par rapport à l'avant-projet, le projet renonce à conserver une disposition spéciale sur les pouvoirs de l'ATPrDM en lien avec les communications transfrontières. Cet article faisait inutilement doublon avec la section 5 de la loi consacrée aux pouvoirs de l'Autorité. Il n'en résulte aucune différence sur le fond. Le devoir d'informer le ou la préposé-e des garanties mises en place et la possibilité pour cet organe de se renseigner au sujet des motifs prévus aux lettres b à e ont été maintenus (cf. art. 15 al. 3).

   3.2. Les publications de données personnelles sur Internet ou sur d'autres plateformes qui sont destinées à informer le public en général ne sont pas assimilées à une communication de données à l'étranger (art. 15 al. 4), quand bien même ces informations peuvent aussi être consultées à l'étranger. Cette règle se justifie afin d'éviter l'application de mesures disproportionnées à des situations qui n'en ont pas besoin. Toutefois, il va de soi que de telles publications correspondent à un traitement de données et qu'elles doivent satisfaire aux règles ordinaires de la loi sur la protection des données.

4. Les restrictions à la communication de données personnelles formulées à l'article 16 du projet restent globalement inchangées par rapport à la loi actuelle (comp. : art. 11 LPrD). La licéité d'une communication dépend non seulement du respect des principes généraux de protection des données, mais également de l'absence de restrictions au sens du présent article. La règle vaut aussi bien pour les communications de données ordinaires que pour les communications de données à l'étranger.

5. L'article 17 du projet réserve expressément certaines règles provenant d'autres législations qui peuvent déroger en partie aux règles de la loi sur la protection des données. A titre d'exemple, les règles sur la communication des données du contrôle des habitants prévues à l'article 17 LCH se suffisent à elles-mêmes et n'impliquent pas de demander en supplément son accord à la personne concernée comme pourrait l'exiger l'article 14 al. 3 du projet. D'autres lois peuvent naturellement aussi déroger à la LPrD, mais celles qui sont citées ici constituent deux exemples clairs par leur importance.

### *Art. 18 à 21, Externalisation*

1. Les articles 18 à 21 reprennent quasiment à l'identique les bases légales sur l'externalisation du traitement de données telles qu'introduites par la loi du 18 décembre 2020 adaptant la législation cantonale à certains aspects de la digitalisation (ROF 2020_195). Pour rappel, ces bases légales ont été introduites suite à un projet pilote mené entre 2018 et 2020 (ROF 2018_112). Depuis leur entrée en vigueur le 1er mars 2021, elles ont fourni un cadre clair et utile à l'utilisation de services en nuage (services *cloud*) par les autorités cantonales. Elles ont permis le développement de pratiques harmonisées et cohérentes tant sur le plan technique que contractuel.

2. A l'heure actuelle, seuls quelques cantons disposent de règles spécifiques concernant l'usage du *cloud computing* (Glaris, Lucerne, Zurich). Au niveau de la Confédération et des autres cantons, *le cloud computing* est généralement assimilé à un simple cas de sous-traitance et, partant, soumis aux règles y relatives (cf. art. 37 du projet). Mais comme ces règles sont relativement modestes et qu'elles ne tiennent pas compte des spécificités propres au *cloud computing* (localisation ubiquitaire des données, caractère généralement durable de l'externalisation, aspects contractuels spécifiques, maîtrise et responsabilité partagées sur les données, législation étrangère…), il en résulte qu'elles ne sont pas vraiment adaptées pour réguler l'usage de cette technologie. En outre, la licéité du recours au *cloud computing* basée sur les règles en matière de sous-traitance n'est pas admise unanimement à ce jour. Un recours à ce sujet déposé par un particulier contre la Chancellerie fédérale est en ce moment pendant devant le Tribunal administratif fédéral[6]. Cette situation crée une forte insécurité juridique qui pèse sur les responsables du traitement, qui ne savent pas s'ils risquent ou non d'engager leur responsabilité en cas de recours à une solution *cloud*. Pour ces raisons, le Conseil d'Etat a proposé de réguler l'usage du *cloud computing* dans le canton de Fribourg au moyen de règles qui non seulement autorisent cet usage, mais qui en fixent également les prérequis techniques et juridiques. L'externalisation au moyen d'une solution *cloud* est ainsi considérée comme une forme qualifiée de sous-traitance qui répond à un corpus de règles spéciales ayant pour but d'appréhender cette technologie de la meilleure manière possible.
3. L'article 18 constitue la base légale permettant aux collectivités publiques de procéder à l'externalisation du traitement de leurs données personnelles (al. 1). Il fixe un cadre géographique aux lieux de traitement autorisés. Seul le territoire suisse ou celui d'un Etat dont la législation en matière de protection des données est jugée adéquate au sens de l'article 15 al. 1 sont éligibles à une externalisation (al. 2). La réserve de l'article 54 Cst./FR est prévue pour le cas où l'externalisation du traitement équivaudrait à une délégation complète d'une tâche de l'Etat (p.ex. si un service *cloud* fourni par un prestataire externe venait à rendre lui-même une décision sans que l'administration n'intervienne). Ce type de situation n'est pas couvert par cet article et nécessiterait, en vertu de la Constitution, l'adoption d'une base légale spécifique (al. 3). L'exigence d'un rapport sur l'externalisation à remettre tous les deux ans à la Commission des finances et de gestion a été expressément demandée par le Grand Conseil lors des débats parlementaires relatifs à la loi adaptant la législation à certains aspects de la digitalisation (al. 4). Elle a été reprise telle quelle dans le projet.
4. Les règles sur la responsabilité sont énoncées à l'article 19.

   4.1. Le principe de base est que l'organe qui externalise le traitement de ses données sur les infrastructures d'un sous-traitant reste responsable de leur conservation, de leur exploitation et de leur confidentialité (al. 1). La disposition énonce un certain nombre de points importants à prendre en considération. En particulier, l'organe qui externalise le traitement de ses données doit choisir son sous-traitant avec soin, l'instruire sur les tâches à accomplir au moyen d'un contrat suffisamment précis et surveiller qu'il respecte les éléments du contrat.

   4.2. On peut donner ici, à titre d'exemple, une *check-list* des différents éléments qu'un contrat d'externalisation devrait, selon les circonstances, inclure :

   a) l'objet, la nature et la finalité du traitement ;

   b) les catégories des données traitées et leur degré de confidentialité ;

   c) l'emplacement des serveurs assurant l'hébergement des données ;

   d) les mesures mises en place afin de garantir la sécurité et la confidentialité des données ;

   e) les personnes ou les catégories de personnes ayant accès aux données ou aux applications concernées ;

   f) les droits et les possibilités de contrôle ;

[6] https://www.bvger.ch/bvger/fr/home/medias/medienmitteilungen-2022/public-clouds.html. Dernière vérification effectuée le 15 mars 2023.

g) l'interdiction faite au sous-traitant de sous-traiter à son tour le traitement de données sans l'accord préalable de l'autorité responsable et la signature d'un contrat d'externalisation posant les mêmes exigences que celui passé entre l'autorité responsable et le sous-traitant ;

h) les devoirs d'annonce du sous-traitant en cas d'incident, de perte ou de vol de données, ou en cas de demandes émanant d'autorités étrangères ;

i) les possibilités de récupérer les données et les applications concernées en cours de contrat ;

j) les processus à respecter en cas de résiliation du contrat, en particulier la restitution des données ainsi que leur destruction chez le sous-traitant ;

k) dans la mesure du possible, l'applicabilité du droit suisse et la désignation d'un for en Suisse en cas de litige.

Ces éléments pourront toutefois évoluer avec le temps et en fonction des types d'externalisation.

4.3. Par rapport à la loi actuelle, l'article 19 al. 1 let. b ch. 4 mentionne dorénavant les droits et les possibilités de contrôle sur le sous-traitant sans préciser à qui ces droits doivent revenir. Il s'agit alors non plus seulement des droits de contrôle de l'Autorité de surveillance, comme le prévoit la loi actuelle, mais aussi du responsable du traitement. Différentes possibilités de contrôle peuvent être envisagées en fonction des sous-traitants. En pratique, peu nombreux sont les sous-traitants qui acceptent une inspection sur site de leurs infrastructures. D'une part, cette solution les expose à un risque de violation des secrets commerciaux. D'autre part, elle peut également s'avérer peu concluante suivant la taille du sous-traitant. Souvent, les contrats *cloud* prévoient que le sous-traitant se fait régulièrement auditer par une entreprise spécialisée dans ce type d'audit et au bénéfice de connaissances et de moyens très poussés. Les résultats de l'audit sont alors transmis au responsable du traitement. Il va sans dire qu'ils sont alors aussi accessibles à l'Autorité de surveillance.

4.4. Au sein de l'administration cantonale, le respect des dispositions en matière d'externalisation est assuré conjointement par l'organe compétent à raison de la matière et le SITel (al. 2). Cette manière de procéder permet de développer une pratique cohérente et autant que possible uniforme. Le SITel veille notamment que le processus d'externalisation suive les étapes indiquées et que le contrat d'externalisation contienne toutes les clauses nécessaires pour garantir la sécurité et la protection des données personnelles externalisées. La disposition réserve toutefois le cas des organes publics qui gèrent leur informatique de façon autonome, à l'instar de l'Université, de l'Office de la circulation et de la navigation ou encore de l'Hôpital fribourgeois. Ces organes sont seuls responsables de l'externalisation de leurs données et de leurs outils informatiques.

4.5. Certaines solutions de *cloud computing* ne sont pas limitées à un seul organe d'une collectivité publique mais peuvent s'étendre à plusieurs d'entre eux, voire à tous. Il est évident alors que chaque organe public concerné ne peut pas personnellement s'assurer que le sous-traitant respecte ses engagements. Dans ce cas, le Conseil d'Etat désigne un organe principalement responsable (al. 3). Il s'agit, en principe, de l'organe qui introduit la solution et en impose l'utilisation à l'intérieur de l'Etat. Il devient alors responsable de la solution pour l'ensemble de l'administration. Il répond de manière générale de sa conformité avec les exigences de la protection des données ; il est tenu de fournir des instructions d'utilisation et un support de première ligne aux autres utilisateurs de l'Etat concernant son fonctionnement et c'est lui aussi le principal interlocuteur du fournisseur au sein de l'administration. Les autres organes utilisateurs sont quant à eux responsables uniquement des opérations de traitement qu'ils accomplissent eux-mêmes au moyen de la solution. En cas de problème qu'ils ne peuvent pas résoudre eux-mêmes, ils doivent s'adresser à l'organe principalement responsable qui va s'adresser, si nécessaire, au fournisseur de la solution. Lorsque le service principalement responsable n'est pas le SITel, l'article 19 al. 2 reste applicable cumulativement avec l'article 19 al. 3. La mise en œuvre et le suivi des règles en matière d'externalisation sont assumés conjointement par l'organe principalement responsable et par le SITel. Lorsque l'organe principalement

responsable est le SITel lui-même, l'article 19 al. 2 n'a logiquement plus d'objet. A titre d'exemple de solution visée par cette disposition, on peut citer la suite M365 fournie par Microsoft. Elle a été déployée par le SITel pour l'ensemble des services de l'administration. Le SITel en a été désigné organe principalement responsable.

5. Les mesures de sécurité à mettre en place lors d'une externalisation sont réglées de manière générale à l'article 20. La loi ne cite toutefois volontairement pas de mesures spécifiques, celles-ci devant être prévues au cas par cas dans le contrat d'externalisation. Cela est justifié pour deux raisons. D'une part, chaque type de traitement de données susceptible d'être externalisé ne répond pas nécessairement aux mêmes besoins de sécurité. D'autre part, la loi doit rester technologiquement neutre afin de ne pas entraver l'utilisation de techniques et de technologies additionnelles ou futures. Même si les mesures de sécurité à mettre en place poursuivent généralement plusieurs buts différents, l'alinéa 2 rappelle le besoin d'accorder une place particulière à la protection des personnes concernées et de leurs droits fondamentaux. Pour prévenir le risque que l'Etat ne se trouve complètement paralysé en cas de dysfonctionnement survenant chez le fournisseur de service *cloud*, la loi impose finalement l'adoption de mécanismes de remplacement en cas d'incident si les données concernées sont indispensables au fonctionnement de l'Etat (al. 3). Ces mécanismes doivent servir à minimiser autant que faire se peut les conséquences d'une défaillance du fournisseur de service *cloud* entrainant la perte ou l'indisponibilité prolongée des données. Comme de tels inconvénients peuvent aussi entrainer des conséquences importantes pour la personne concernée, il se justifie d'introduire une telle règle également dans la loi sur la protection des données.

6. L'externalisation de données sensibles et de secrets est traitée à l'article 21 du projet.

   6.1. Les mesures prescrites reprennent les recommandations de la Conférence des préposé-e-s à la protection des données (PRIVATIM). Ces dernières prévoient la mise en place de mesures supplémentaires de sécurité :

   > Les données doivent être chiffrées et le chiffrement doit être réalisé par l'organe public. Les clés ne doivent être disponibles que pour l'organe public. Elles doivent être protégées de la perte et de la soustraction, ainsi que de l'utilisation et de la prise de connaissance abusives (al. 1).

   > Un chiffrement peut être envisagé chez le fournisseur de service *cloud* seulement si cela ne fait pas encourir des risques inacceptables aux droits fondamentaux des personnes concernées. Dans ce cas, il faut tenir compte du niveau auquel le chiffrement a lieu (application, banque de données ou disque dur). Le fournisseur de service *cloud* peut conserver les clés de déchiffrage s'il s'engage par contrat à les utiliser uniquement avec le consentement exprès de l'organe public. Les accès doivent, en outre, être tracés et consignés dans un journal des accès. Finalement, le fournisseur de service *cloud* doit protéger les clés de déchiffrage de la perte et de la soustraction, ainsi que de l'utilisation et de la prise de connaissance abusives. Il doit aussi garantir que les données ne soient pas compromises lors du processus de chiffrement (al. 2).

   > Pour les secrets, les exigences sont globalement les mêmes. Il faut toutefois dans ce cas veiller en plus à ce que le fournisseur de service *cloud* puisse être qualifié d'auxiliaire du détenteur du secret (al. 3). Cette qualification qui découle du droit pénal est prévue à l'article 321 CP pour le secret professionnel et sera introduite en cours d'année 2023 à l'article 320 CP pour le secret de fonction[7]. Sont visés les professionnel-le-s qui assistent une personne soumise au secret dans l'accomplissement de ses tâches. La transmission d'informations soumises au secret à un auxiliaire n'est pas punissable. Dans un arrêt concernant le secret de l'avocat, le Tribunal fédéral a jugé qu'un fournisseur de service *cloud* peut être considéré comme un auxiliaire de l'avocat[8].

[7] Modification de l'article 320 CP introduite lors de l'adoption de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI), in : RO 2020 232.

[8] ATF 145 II 229, consid. 7.3.

6.2. La disposition prévue retranscrit ces exigences au niveau de la loi dans un langage qui est neutre sur le plan de la technologie.

### *Art. 22, Essais pilotes*

1. La disposition sur les essais pilotes a fait l'objet de certaines adaptations. Son contenu a été réparti entre la LCyb pour les projets pilotes généraux et la LPrD pour les projets pilotes incluant certains traitements de données personnelles présentant un caractère plus délicat. Si ces traitements de données ont lieu dans le cadre d'un projet pilote, leur traitement pourra momentanément reposer sur une ordonnance du Conseil d'Etat plutôt que sur une loi adoptée par le Grand Conseil.
2. Les conditions de fond à la réalisation d'un projet pilote sont décrites aux articles 35 à 35b LCyb. Il faut, en particulier, une tâche à accomplir, un besoin d'expérimentation, la nécessité d'une phase d'essai, la constitution d'un dossier complet, l'adoption par le Conseil d'Etat d'une ordonnance expérimentale d'une durée limitée et un rapport d'évaluation rétrospective. L'article 21 p-LPrD ajoute des conditions particulières pour les projets pilotes qui incluent le traitement de données sensibles ou d'autres types de traitement présentant un risque plus élevé d'atteinte aux droits fondamentaux. D'une part, le dossier du projet pilote et le rapport d'évaluation qui clôture la phase pilote doivent obligatoirement contenir une partie consacrée au traitement des données personnelles ainsi qu'à leur protection (al. 2). Lors de la constitution du dossier du projet, il s'agit d'identifier les risques induits par le projet pilote et les mesures à prendre pour les réduire. A la fin du projet pilote, au moment de l'évaluation, il faut analyser rétrospectivement si les risques identifiés ont pu ou non être suffisamment contenus par les mesures prises, si d'autres risques sont apparus qui n'avaient pas été identifiés, si ces risques ont pu être contenus et, plus généralement, de mettre en balance les risques résiduels avec les avantages constatés par le projet. D'autre part, l'Autorité de surveillance doit obligatoirement être consultée au moment de la constitution du dossier et au moment de l'évaluation rétrospective (al. 3). L'Autorité reçoit les deux documents avant leur transmission au Conseil d'Etat et est invitée à se prononcer. Sa prise de position est ensuite communiquée au Conseil d'Etat.
3. Il va sans dire qu'en dehors de ces deux phases, l'Autorité de surveillance conserve toute possibilité d'intervenir durant la phase pilote. En pratique, des échanges ponctuels, voire réguliers, sont même encouragés dans les limites des ressources de l'Autorité.

### *Art. 23, Archivage*

Dès lors qu'elles présentent une valeur archivistique, les données personnelles traitées par les pouvoirs publics sont soumises à la législation sur l'archivage. Elles ne peuvent pas être effacées ou détruites (cf. commentaire de l'article 10). Pour que l'obligation de supprimer les données qui ne poursuivent plus aucune finalité conserve un sens, il conviendra de mettre en place des mécanismes permettant de déterminer la valeur archivistique d'un document dans des délais raisonnables.

### *Art. 24, Effacement et destruction de données*

1. Sous réserve des données qui ont été identifiées comme présentant une valeur archivistique, les données personnelles conservées auprès d'un organe public doivent être effacées ou détruites lorsque leur conservation ne poursuit plus aucune finalité. Il en résulte le devoir de procéder périodiquement à un examen des données personnelles conservées.
2. Pendant la durée d'utilisation du support par un organe public – soit aussi longtemps que celui-ci est sous le contrôle de l'administration – les données personnelles qui y sont conservées doivent être effacées régulièrement conformément à l'alinéa 1er. Au moment de recycler ou de remplacer du matériel informatique, le responsable du traitement devra s'assurer qu'il n'existe pas un risque que des données sensibles ayant été effacées puissent être retrouvées et exploitées par une personne non-autorisée. Si tel est le cas, le support en question (p. ex. le disque dur) devra être physiquement détruit (al. 2). La destruction des supports est de la responsabilité du SITel.

#### *Art. 25, Vidéosurveillance*

Pas de commentaire.

### 2.2.3 Section 2.3 : Traitement de données à des fins ne se rapportant pas à la personne

#### *Art. 26, Règles*

L'allégement des exigences en matière de protection des données s'agissant des traitements à des fins ne se rapportant pas à la personne se justifie du fait que ces traitements présentent des risques moindres dans la mesure, précisément, où ils ne se rapportent pas à des personnes et où certaines prescriptions spécifiques sont respectées. Par ailleurs, ces prescriptions tiennent compte de l'intérêt public que représentent la recherche, la planification et la statistique.

## 2.3 Section 3, Droits de la personne concernée

#### *Art. 27 à 30, Droit d'accès*

1. Le droit d'accès (art. 27) est et reste l'institution centrale du droit de la protection des données. Sans droit d'accès, la personne concernée ne serait pas en mesure d'exercer ses droits en la matière. Seul celui ou celle qui a connaissance d'un traitement de données le ou la concernant est à même, le cas échéant, d'en vérifier le but ou de demander la rectification ou la suppression des données inexactes ou sans lien avec le but du traitement. Le débiteur du droit d'accès est toujours le responsable du traitement au sens de l'article 4 al. 1 let. h. Le fait que celui-ci confie le traitement à un tiers ne change rien à cet égard (al. 3).
2. Le droit d'accès est la manifestation la plus concrète du droit fondamental à la protection des données. Il appartient à toute personne qui fait l'objet d'un traitement et ne dépend d'aucun intérêt particulier. Cela signifie qu'il n'y a aucune restriction liée à la nationalité, au domicile ou à l'âge, voire à la personnalité du demandeur ou à ses motivations et à l'usage qu'il compte faire de ses données. Le demandeur n'a, en outre, pas à motiver sa demande. La seule obligation qui lui incombe est de fournir son identité afin que seules ses propres données lui soient effectivement transmises (art. 28 al. 1). Pour rappel, il existe une règle particulière en matière de droit d'accès à l'article 60 al. 3 LSan. Pour les demandes d'accès auprès de professionnel-le-s de la santé, le responsable du traitement (en principe le médecin traitant ou la médecin traitante) peut proposer à la personne concernée qu'elle consulte ses données en présence d'un spécialiste de son choix. Il ne s'agit cependant que d'une proposition que la personne concernée est libre d'accepter ou de refuser.
3. Le droit d'accès n'est pas absolu. L'article 29 du projet énonce les conditions auxquelles il peut être restreint. L'invocation d'un motif de restriction au droit d'accès doit toutefois rester l'exception. Elle ne peut avoir lieu que de manière restrictive sur la base d'une pesée des intérêts en présence et conformément au principe de proportionnalité. Par rapport à l'avant-projet, le projet prévoit deux motifs de restriction supplémentaires. Le premier, la loi, est mentionné à titre indicatif dans la mesure où une loi peut, de manière générale, toujours déroger à une autre loi. Le second, l'invocation du caractère abusif de la demande, est un alignement sur le droit fédéral et celui des autres cantons. Il correspond à une concrétisation de l'abus de droit. Toutefois, il ne pourra, en pratique, être invoqué que restrictivement, si l'abus est manifeste.
4. L'article 30 n'est pas directement une manifestation du droit d'accès de la personne concernée, mais énonce divers principes concernant la consultation de certaines de ses données après la mort. Même si on peut discuter son emplacement, celui-ci peut néanmoins se justifier pour des raisons didactiques et aussi de systématique. Dans tous les cas, l'élément essentiel qui ressort de cette disposition est la pesée des intérêts qui doit être faite au moment de décider de transmettre à des tiers des données du défunt ou de la défunte.

#### *Art. 31, Opposition à la communication de données personnelles*

1. Le droit d'opposition (ou droit de blocage) permet à la personne concernée de s'opposer par avance à la communication de certaines données la concernant. Il fait partie des prétentions que le droit de la protection des données reconnaît aux personnes concernées de manière générale sans égard au type de données visées (cf. art. 20 LPD et 37 n-LPD ; voir aussi art. 21 RGPD ; art. 9 § 1 let. d Convention STE 108+).

2. Selon le droit actuel, le droit de blocage est uniquement prévu pour les données du registre des habitants à l'article 18 LCH. En 2003, l'ancienne Commission fédérale de la protection des données a rendu un jugement concernant le canton de Fribourg dans lequel elle a déclaré que le fait de limiter le droit d'opposition à certaines catégories de données uniquement est contraire au droit de la protection des données (Jugement de l'ancienne Commission fédérale de la protection des données du 22 mai 2003, in JAAC 68.69). Le projet prévoit par conséquent l'introduction d'un droit d'opposition élargi qui ne dépend pas du type de données en cause.

3. Le droit d'opposition n'est toutefois ni général, ni absolu. Premièrement, il ne peut porter que sur des données préalablement définies par la personne concernée (al. 1 *in fine*). Il n'existe donc pas de droit de blocage général portant sur l'ensemble des données d'une personne. Deuxièmement, le blocage des données peut être mis en échec aux conditions énoncées à l'alinéa 2 let. *a* à *c*. Tel sera le cas à chaque fois que la communication est expressément ordonnée par la loi (let. *a*), lorsque le blocage de la communication risque de sensiblement entraver l'organe public dans l'accomplissement de ses tâches (let. *b*) ou qu'il aurait pour conséquence d'empêcher une tierce personne de défendre ses intérêts légitimes alors qu'aucun obstacle juridique ne s'oppose à la communication (let. *c*). Dans ce dernier cas, l'autorité saisie d'une requête de communication doit trancher entre refuser la communication à celui ou celle qui en a fait la demande ou lever le droit d'opposition de la personne concernée. Comme ce choix s'accompagne nécessairement de conséquences juridiques pour chacune des deux parties, l'autorité saisie doit se prononcer au moyen d'une décision qui est sujette à recours (al. 3).

4. L'alinéa 4 réserve les règles concernant le devoir d'informer des autorités et l'accès à des documents officiels prévus la LInf. Par défaut, le droit de blocage au sens de la LPrD ne peut pas à lui seul constituer un motif de restriction face aux exigences de transparence de l'administration. En cas de communication active des autorités ou de demande d'accès à un document officiel contenant des données personnelles pour lesquelles la personne concernée a fait valoir son droit de blocage, le traitement de la demande d'accès devra se faire conformément aux règles prévues aux articles 11 et 26 ss LInf.

### *Art. 32, Portabilité des données*

1. Le droit à la portabilité des données ne faisait volontairement pas partie de l'avant-projet car il était jugé prématuré et peu adapté au traitement des données dans le domaine public. Néanmoins, il a été ajouté dans le projet afin de disposer d'une législation complète en matière de protection des données et afin d'anticiper de nouvelles évolutions possibles.

2. Tel qu'il est formulé, le droit à la portabilité des données n'est cependant pas directement justiciable, mais nécessite d'être concrétisé dans la législation spéciale ou d'être proposé volontairement par le responsable du traitement. La raison à cela est que toutes les bases de données ne permettent pas de procéder sur demande à une extraction automatisée d'une partie de leur contenu. Pour parvenir à un tel résultat, il faut un certain nombre de prérequis techniques. Il faut que les données soient structurées et qu'elles soient enregistrées dans des formats adaptés. Or ces prérequis ne sont pas appropriés pour toutes les bases de données. C'est la raison pour laquelle l'article 32 se limite à définir un cadre au droit à la portabilité des données.

### *Art. 33, Actions défensives*

1. L'alinéa 1er énonce les trois moyens défensifs traditionnels face à un traitement de données illicite. Il s'agit des mêmes moyens prévus en droit civil dans le domaine de la protection de la personnalité.

2. L'expression « quiconque a un intérêt digne de protection » en début de phrase reprend celle prévue à l'article 41 n-LPD. Elle ne vise pas uniquement la personne directement concernée par le traitement effectif de ses données. En plus de cette dernière, certaines associations peuvent, en outre, aussi être habilitées à invoquer l'une ou l'autre prétention prévues à l'article 30 al. 1, lorsqu'elles agissent pour défendre leurs intérêts propres ou ceux de leurs membres (« recours égoïste » ; en allemand « egoistische Verbandsbeschwerde »). Pour savoir si une personne dispose d'un intérêt digne de protection lui permettant de s'opposer à un traitement de données, il est possible de se référer à la jurisprudence du Tribunal fédéral (not. ATF 147 I 280, consid. 6.2).

3. L'alinéa 2 énonce différents moyens propres au droit de la protection des données qui peuvent être invoqués dans un cas concret afin de remédier à une atteinte provoquée par un traitement illicite de données. La personne peut, en particulier, demander de supprimer ou de rectifier des données inutiles ou inexactes ; elle peut aussi demander l'ajout d'une mention du caractère litigieux de certaines données, lorsque ni leur exactitude, ni leur inexactitude ne peut être établie. La communication à des tiers ou la publication de la suppression, de la rectification de données personnelles ou de l'ajout de la mention de leur caractère litigieux font également partie des moyens à disposition. La nouveauté par rapport au droit actuel est l'introduction d'un droit à la limitation du traitement. Moins radicale que la rectification ou que la suppression des données, la limitation du traitement permet de geler temporairement les possibilités de traitement liées à certaines données généralement dans l'attente de clarification soit sur leur exactitude, soit sur la licéité des traitements querellés. Pendant la mesure, le responsable du traitement peut – respectivement doit – continuer de conserver intactes les données visées, mais il ne peut plus les traiter pour des fins nouvelles.
4. L'alinéa 3 rappelle le principe d'intégrité des fonds d'archives ou des fonds ouverts au public, y compris lorsqu'ils contiennent des données personnelles. Ces fonds et leur contenu ne peuvent être ni détruits ni rectifiés. Dans certaines situations, leur accès peut toutefois être restreint et/ou il peut être ajouté une note dans laquelle la personne concernée ou un proche réfute, voire éventuellement complète, des données la concernant.

#### *Art. 34, Procédure et voies de droit*

Depuis la révision de la LPrD de 2008, toutes les décisions rendues par les organes publics en application de la présente section doivent systématiquement être transmises à l'Autorité de surveillance. Cela lui permet d'en vérifier la conformité à la loi et, en cas de besoin, de recourir. Ce système peut cependant engendrer une atteinte aux droits fondamentaux des personnes concernées si ces dernières ne souhaitent pas pareille communication. C'est pourquoi, par rapport à la loi actuelle, le projet introduit la possibilité pour les intéressé-e-s de s'opposer à la communication des décisions qui les concernent.

#### *Art. 35, Réparation du dommage et du tort moral*

La violation des dispositions de la loi sur la protection des données peut constituer un acte illicite au sens de de l'article 6 al. 1 LResp. Elle peut donner lieu à réparation aux conditions fixées dans la loi.

### 2.4 Section 4, Mise en œuvre de la protection des données

#### *Art. 36 et 37, Responsabilités*

1. L'article 36 pose le principe selon lequel l'organe public qui traite des données personnelles est responsable de leur protection et de leur sécurité (al. 1). Cette règle et les conséquences en découlant sont précisées à d'autres endroits de la LPrD comme dans d'autres types d'actes.
2. La responsabilité d'un traitement de données peut toutefois être partagée entre différents acteurs (al. 2) qui en deviennent alors co-responsables. En de telles circonstances, il importe que le partage des responsabilités soit suffisamment défini entre les acteurs concernés (p. ex. : périmètre, catégories de données, types de traitement *etc.*). Cela peut soit être fait au moyen de la déclaration prévue à l'article 38, soit ressortir d'une ou plusieurs dispositions légales. Dans tous les cas, la répartition des responsabilités en interne n'a aucune influence sur la situation des personnes concernées qui sont toujours admises à faire valoir l'ensemble de leurs droits et de leurs prétentions auprès de l'Etat.
3. L'article 37 règle les questions de responsabilité lorsqu'un organe public fait appel à un sous-traitant. Par rapport à l'avant-projet, la disposition a subi un alignement sur le droit fédéral. On y retrouve ainsi les conditions ordinaires en Suisse relatives à ce domaine. Une précision a toutefois été ajoutée à l'alinéa 5. Elle prévoit que, sauf disposition contraire, il n'y a pas de sous-traitance entre plusieurs organes appartenant à une même collectivité. On préfère dans ce cas l'application des règles sur la co-responsabilité. Cela n'a pas d'impact sur les personnes concernées, puisque la responsabilité reste de toute manière celle de l'Etat. Mais cela évite d'avoir à élaborer des constructions juridiques compliquées et peu utiles.

4. L'externalisation de données constituant dans le projet une forme de sous-traitance qualifiée, elle fait l'objet de règles spéciales prévues dans la section 2 de la loi consacrée aux formes particulières de traitement (cf. art. 18 à 21). Les règles de base prévues à l'article 37 restent cependant applicables aussi longtemps qu'elles ne contredisent pas les règles spéciales en matière d'externalisation.

### *Art. 38 à 39, Registre des activités de traitements et déclarations de traitement*

1. La déclaration des activités de traitement et le registre des activités de traitement sont des instruments de gouvernance en matière de protection des données qui assurent à la fois la transparence et le contrôle des activités de traitement des organes publics. Même si des évolutions sont probables, il faut partir de l'idée que cette fonction continuera d'être assumée par l'actuel Registre des fichiers (REFI) tenu par l'ATPrDM.
2. Le remplacement du terme « fichier » par « activité de traitement » correspond à une adaptation terminologique et ne devrait pas amener de changements pratiques majeurs. En particulier, il n'est pas question de déclarer chaque opération de traitement individuellement. Le terme fichier est jugé obsolète car les données nécessaires à l'accomplissement d'une tâche ne sont aujourd'hui plus nécessairement stockées dans un espace délimité mais peuvent être entreposées à différents endroits alors qu'elles servent à une même activité. C'est pourquoi le législateur fédéral, la Convention STE 108+ et les nouvelles lois cantonales ont remplacé le terme « fichier » par « activité de traitement ». Cela ne veut pas dire pour autant que les deux termes soient forcément identiques à 100 % et qu'ils recouvrent exactement la même réalité. Même s'il ne devrait pas en résulter une augmentation des déclarations, la déclaration des activités de traitement exigera qu'il faudra à l'avenir réfléchir non plus par rapport au lieu de stockage mais par rapport à l'activité devant être accomplie (généralement celle prévue par la loi). Il peut donc en résulter certaines différences.
3. L'article 38 énonce la liste des informations que le responsable du traitement doit fournir au moment de procéder à la déclaration. L'article 39 fixe un certain nombre d'exceptions à l'obligation de déclarer. Ces dispositions sont largement similaires à ce que prévoit la LPrD actuellement.
4. Le registre des activités de traitement est tenu par l'ATPrDM[9]. Il est public et consultable gratuitement. Le projet renonce toutefois à préciser qu'il doit être publié en ligne dans la mesure où cela correspond déjà à la pratique actuelle et qu'on n'imagine pas qu'il pourrait en être autrement. Il renonce aussi à préciser que les communes doivent conserver une liste de leurs traitements en plus de les annoncer à l'ATPrDM.
5. L'avant-projet prévoyait qu'un traitement de données devait obligatoirement être annoncé à l'Autorité de surveillance avant de pouvoir démarrer (cf. art. 38 al. 1 ap-LPrD). Cette obligation a été abandonnée, car elle n'est pas réalisable en pratique. Elle aurait aussi constitué une mesure totalement unique en Suisse.

### *Art. 40, Mesures organisationnelles et techniques*

1. L'article 40 qui évoque les mesures organisationnelles et techniques à mettre en place a été fusionné dans le projet avec l'article 42 de l'avant-projet qui introduisait les principes de la protection des données dès la conception et par défaut (*Privacy by design* et *Privacy by default*). Ces derniers consacrent une approche proactive de la protection de la vie privée tout au long du processus de traitement des données.
2. Les responsables du traitement doivent prendre tout au long du cycle de vie des données les mesures organisationnelles et techniques appropriées à leur situation, aux traitements qu'ils accomplissent et au type de données qu'ils traitent. Différents critères doivent être pris en considération. Il s'agit non seulement de la confidentialité mais aussi de la disponibilité, de l'authenticité, de l'intégrité, de la traçabilité et de la pérennité. Des indications plus précises à ce sujet figureront dans la législation sur la sécurité de l'information actuellement en cours de préparation et auquel renvoie notamment l'alinéa 2.

[9] Le Registre des Fichiers (ReFi) est accessible en ligne sur la page : https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/registre-des-fichiers-refi.

3. Conformément à l'approche fondée sur les risques, la loi ne fixe pas directement de mesures spécifiques à mettre en place mais reprend à son compte le principe d'« *accountability* » que l'on retrouve dorénavant dans la plupart des lois modernes de protection des données (art. 4 § 4 de la Directive (UE) 2016/680 ; art. 5 § 2 RGPD et art. 10 § 1 de la Convention STE 108+). Difficilement traduisible en français, ce nouveau principe implique pour les responsables du traitement deux choses :

   a) Mettre en œuvre des mesures effectives, appropriées et adaptées aux circonstances visant à garantir la protection et la sécurité des données personnelles qu'ils traitent. Outre la mise en place de solutions techniques, il peut s'agir de mesures de sensibilisation et de formation, de mesures de protection des locaux ou encore de mécanismes pour limiter les conséquences d'une perte ou d'un vol de matériel fixe ou mobile.

   b) Etre en mesure de démontrer l'existence et la mise en œuvre de ces mesures au travers d'une documentation adaptée (cf. al. 4). L'ampleur du devoir de documenter dépend des circonstances. Il peut prendre, en particulier, les formes suivantes : simple liste régulièrement actualisée des mesures, charte, politique, concept SIPD, règlement d'utilisation, *etc*.

### *Art. 41 et 42, Analyse d'impact relative à la protection des données*

1. L'analyse d'impact relative à la protection des données est un outil important pour la responsabilisation des auteurs de traitement. Elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité à la loi sur la protection des données. L'analyse d'impact doit être menée par le responsable du traitement avant la mise en œuvre du traitement ; elle doit ensuite être régulièrement évaluée pour s'assurer de son actualité tout au long de la vie du traitement.

2. A l'instar de ce que prévoient le droit européen (art. 27 § 1 Directive (UE) 2016/680 et art. 35 § 1 RGPD), la Convention STE 108+ (art. 10 § 2) et la n-LPD (art. 22), l'analyse d'impact est obligatoire pour les traitements susceptibles d'engendrer des risques élevés pour les droits et les libertés des personnes concernées (art. 41 al. 1). Le risque doit être analysé au cas par cas en termes de gravité et de vraisemblance. La loi fournit à titre d'exemple une liste de cas pour lesquels la réalisation d'une telle analyse est obligatoire (al. 2). Le contenu minimum de l'analyse d'impact est décrit à l'article 41 al. 3. Sa réalisation doit être menée sans formalités excessives dans le respect du principe de proportionnalité.

3. Lorsqu'il ressort de l'analyse d'impact que le traitement envisagé présente un risque élevé pour les droits des personnes concernées et nécessite de ce fait de prendre des mesures de protection particulières, le responsable du traitement doit consulter l'Autorité de surveillance avant d'être en droit de débuter le traitement (art. 42 al. 1). Cette dernière peut communiquer au responsable du traitement ses éventuelles objections et recommandations concernant le traitement envisagé (al. 2). Selon le projet, l'Autorité dispose d'un délai de deux mois, prolongeable d'un mois, pour rendre sa prise de position. Sans retour de la part de l'Autorité, le responsable du traitement peut partir de l'idée que l'Autorité renonce à se positionner et qu'il peut donc démarrer le traitement. Cela n'empêche toutefois pas l'Autorité d'intervenir ultérieurement.

4. Le responsable du traitement est libre de mettre en pratique ou non les recommandations formulées par l'Autorité de surveillance, mais il doit dans tous les cas l'informer des suites données au plus tard au moment de débuter le traitement (al. 3). Si le responsable du traitement décide de ne pas suivre les recommandations de l'Autorité et que cette dernière estime que le traitement n'est pas conforme aux exigences de la protection des données, elle peut alors faire usage de tous les pouvoirs mis à sa disposition conformément aux articles 56 ss. Les mêmes règles s'appliquent au niveau fédéral.

### *Art. 43 et 44, Violations de la sécurité des données*

1. Les mesures à prendre en cas d'incident entrainant une violation de la confidentialité, de la disponibilité ou de l'intégrité des données portent sur trois niveaux : *a)* identification de la violation et correction (art. 43 al. 1) ; *b)* consignation de la violation dans un document écrit (art. 43 al. 2) et *c)* lorsque cela est nécessaire, annonce de

la violation au ou à la préposé-e à la protection des données, voire aux personnes concernées (art. 43 al. 3 et art. 44).

2. La loi n'exige pas que tout incident en matière de protection des données soit systématiquement notifié au ou à la préposé-e à la protection des données. Seuls sont visés les incidents entraînant vraisemblablement un risque élevé pour les droits des personnes concernées. Pour qu'un risque élevé soit reconnu, il faut qu'un dommage, par exemple un vol, une usurpation d'identité ou encore une discrimination, soit susceptible de se produire. Il n'est, en revanche, pas nécessaire qu'un nombre minimum de personnes soient concernées.[10] La loi renonce à fixer le délai durant lequel la communication doit avoir lieu. Celui-ci doit toutefois rester aussi bref que possible. Il ne devrait, en principe, pas excéder 72 heures (comp. : art. 30 § 1 Directive (UE) 2016/680 ; art. 33 § 1 RGPD).
3. Lorsque cette mesure s'impose pour des motifs de transparence et/ou pour permettre aux personnes concernées de prendre les mesures utiles à la sauvegarde de leurs intérêts (p. ex., en changeant leur mot de passe, en bloquant un accès ou en prenant contact avec l'autorité), les personnes concernées doivent être averties personnellement de la violation (art. 44 al. 1). En cas d'inaction du responsable du traitement, l'annonce peut aussi être ordonnée par le ou la préposé-e à la protection des données (art. 44 al. 4). Exceptionnellement, le devoir d'annonce aux personnes concernées peut néanmoins être différé ou restreint. Il est aussi possible d'y renoncer aux conditions usuelles (al. 2). Les motifs d'exception ne s'appliquent, en revanche, jamais à l'annonce au ou à la préposé-e si les conditions d'une communication sont remplies. Pour les cas de violations qui touchent un grand nombre de personnes, le projet prévoit la possibilité d'une annonce publique généralement dans un média (al. 3). Dans pareil cas, on veillera à offrir aux personnes concernées la possibilité d'obtenir des informations suffisamment précises par la création d'une page Internet dédiée ou la mise sur pied d'un point de contact.
4. Conformément à l'article 43 al. 4, toute violation de la sécurité des données survenant chez un sous-traitant doit être annoncée au responsable du traitement (peuvent toutefois faire exception les cas bagatelles ne présentant à l'évidence aucun risque pour la ou les personnes concernées). Lorsqu'il est informé d'une telle violation, le responsable du traitement décide, conformément aux règles exposées ci-dessus, s'il y a lieu ou non de notifier la violation au ou à la préposé-e ou aux personnes concernées.

### *Art. 45, Correspondants et correspondantes en matière de protection des données*

1. L'obligation de désigner un correspondant ou une correspondante à la protection des données vient de la volonté de professionnaliser la compréhension et l'application du droit de la protection des données au sein de l'administration cantonale, compte tenu de son caractère transversal et ubiquitaire.
2. Un profil type n'est pas défini même si, au départ, des connaissances de base de la législation sur la protection des données et un certain intérêt pour les questions informatiques semblent incontournables. Cette fonction peut ainsi être occupée par des juristes, des économistes, des personnes issues de l'informatique ou d'autres cadres de l'administration. Vu le caractère nouveau de ce profil, il faudra surtout au départ que les personnes désignées soient disposées à se former et à se perfectionner dans ce domaine et qu'elles s'intéressent à cette matière. Le pendant est qu'il appartiendra à l'administration de donner à ces personnes les possibilités de se former.
3. Contrairement à l'avant-projet, le projet n'impose plus aux services de désigner des correspondants ou correspondantes mais fait remonter cette obligation à l'échelon des Directions. Le Conseil d'Etat pourra néanmoins obliger d'autres organes cantonaux à désigner un tel rôle au sein d'un service lorsqu'il existe un besoin particulier (al. 5). Le but est de mettre sur pied un pôle de compétences de première ligne à même de résoudre les principales questions en matière de protection des données au sein de l'administration. Les personnes désignées seront réunies dans un réseau au sein duquel elles recevront des formations et pourront

[10] MÉTILLE / MEYER, Annonce des violations de la sécurité des données: une nouvelle obligation de la nLPD, in : RSDA 2021 23, p. 26.

échanger des connaissances et des expériences liées à la protection des données (al. 4). Elles pourront aussi, au besoin, solliciter le soutien et des conseils auprès du ou de la préposé-e.

4. Les correspondants ou les correspondantes assument avant toute chose une fonction de conseil et de soutien. Ils ne sont pas une autorité de surveillance mais interviennent principalement à la demande des responsables du traitement eux-mêmes ou si une affaire l'exige (p. ex. s'ils ont vent d'une violation). Toutefois, même si la loi ne l'exige pas, rien ne les empêche d'agir de manière proactive. Cependant, ils ne sont jamais personnellement responsables de la conformité des traitements à la place du responsable du traitement. Dans toutes leurs interventions, leur rôle est uniquement consultatif.

5. L'autonomie reconnue aux correspondants et correspondantes (al. 3) est une condition nécessaire à l'exercice de leur fonction. Pour accomplir efficacement leur rôle, ces personnes doivent pouvoir prendre clairement position à propos des traitements sur lesquels ils interviennent sans limitation d'ordre hiérarchique ni crainte de subir un préjudice.

## 2.5 Section 5, Surveillance

### 2.5.1 Section 5.1 : Autorité de surveillance en matière de protection des données

#### *Art. 46, Autorité de surveillance*

La désignation d'une autorité de surveillance est une condition indispensable du système de contrôle de la protection des données dans une société démocratique. A l'échelon cantonal, cette fonction est assumée par l'Autorité cantonale de la transparence, de la protection des données et de la médiation (en abrégé : ATPrDM ou Autorité de surveillance). Par rapport à la loi actuelle, le projet renonce à prévoir la possibilité pour les communes de constituer leur propre autorité. Outre le fait que cette faculté n'est actuellement utilisée par aucune commune, la pratique a démontré qu'elle posait de nombreuses difficultés. Ce changement n'a soulevé aucune opposition auprès des communes.

#### *Art. 47, Organisation*

1. Le projet modifie partiellement la structure actuelle de l'Autorité de surveillance. Comme c'est le cas aujourd'hui, l'Autorité reste composée d'une Commission élue par le Grand Conseil qui chapeaute les personnes en charge de la transparence, de la protection des données et de la médiation. Ce système permet de concilier la légitimité tirée d'une commission élue par le Grand Conseil et le professionnalisme ainsi que la disponibilité de spécialistes des domaines concernés. Il n'est pas modifié.

2. Toutefois, en comparaison avec la situation actuelle, le projet propose d'abandonner la séparation entre préposé-e à la transparence et préposé-e à la protection des données et de créer à la place un nouveau poste de préposé-e à la transparence et à la protection des données. D'une solution avec deux préposés, on évolue donc vers une nouvelle solution avec plus qu'un ou une préposé-e agissant dans les deux domaines de la transparence et de la protection des données. Initialement, le choix d'instituer une séparation entre les deux fonctions visait à octroyer la même importance à chaque domaine bien qu'ils répondent parfois à des intérêts antagonistes. Globalement, ce système a toujours bien fonctionné et le Conseil d'Etat n'avait pas prévu de le modifier. Mais suite au départ de l'ancienne préposé-e à la protection des données, l'ATPrDM a annoncé vouloir tester un nouveau mode de fonctionnement avec une personne occupant simultanément la fonction de préposé-e à la transparence et à la protection des données, notamment afin d'améliorer l'efficacité du fonctionnement de l'Autorité. L'actuelle préposée à la transparence a dans ce but été nommée préposée à la protection des données *ad interim*. A l'issue d'une période d'essai de trois mois, l'ATPrDM s'est déclarée satisfaite de ce changement et a demandé qu'il puisse être pérennisé dans le cadre de la révision actuelle de la loi. Plusieurs dispositions de la LPrD et de la LInf ont été modifiées dans ce but.

#### *Art. 48, Statut*

1. L'Autorité de surveillance bénéficie d'un statut particulier au sein de l'administration. La garantie d'indépendance qui lui est reconnue (al. 1) est une exigence fondamentale qui figure déjà dans le texte actuel de la loi (art. 29 al. 3 LPrD) et que l'on retrouve de manière générale dans la réglementation suisse et européenne en

matière de protection des données (cf. art. 26 al. 3 LPD et art. 43 al. n-LPD ; art. 42 de la Directive (UE) 2016/680 ; art. 52 du RGPD ; art. 15 § 5 de la Convention STE 108+). Elle suppose des garanties organisationnelles adaptées portant notamment sur la position de l'Autorité au sein de l'administration, sur les ressources dont elle dispose et sur la désignation et le statut juridique du ou de la préposé-e.

2. Pour assurer son indépendance, l'Autorité de surveillance n'est directement soumise à aucune Direction mais est uniquement rattachée administrativement à l'une d'entre elles (al. 2). Elle ne peut donc pas recevoir d'instructions dans l'exercice de ses fonctions. Cette position ne signifie néanmoins pas que l'Autorité serait « hors de l'Etat » comme le serait un particulier ou une organisation privée et qu'elle pourrait s'autogérer intégralement. L'Autorité de surveillance accomplit ses tâches dans les locaux et avec les moyens que l'Etat lui fournit. Comme toute unité administrative, elle est soumise aux règles relatives à l'utilisations de ces locaux et de ces moyens.
3. L'enveloppe budgétaire remise chaque année à l'Autorité lui confère une très grande autonomie d'exécution et de gestion budgétaire. Elle permet à l'Autorité de décider librement de l'utilisation des deniers reçus dans la mesure où ceux-ci sont liés à l'exécution de ses tâches et/ou à son fonctionnement. En respectant les règles générales applicables aux unités administratives, l'Autorité peut acquérir le matériel qu'elle juge utile, s'inscrire à des formations, financer des campagnes de sensibilisation sur des questions de protection des données, de transparence ou de médiation ou encore commander des avis ou des expertises auprès de spécialistes. Dans les limites de l'enveloppe reçue, elle n'a pas besoin d'obtenir une autorisation préalable pour engager une dépense. L'Autorité peut participer à l'élaboration de son propre budget en adressant une proposition de budget au Conseil d'Etat. Cette proposition est alors présentée par la personne à la tête de la Direction à laquelle l'Autorité est rattachée administrativement, qui peut faire valoir son point de vue lors de sa présentation devant le Conseil d'Etat (cf. art. 61 al. 1 let. a LOCEA).

### *Art. 49 et 50, Commission de la transparence, de la protection des données et de la médiation*

1. L'article 49 règle la composition et l'organisation de la Commission cantonale de la transparence, de la protection des données et de la médiation. Cette dernière est un organe pluridisciplinaire réunissant plusieurs métiers et autant de compétences nécessaires à une compréhension la plus large possible des enjeux liés aux domaines d'activité de l'Autorité. Les membres de la Commission sont élus par le Grand Conseil sur proposition du Conseil d'Etat (al. 1). Cette solution qui a fait ses preuves depuis l'entrée en vigueur de la loi actuelle garantit, d'une part, l'indépendance de l'Autorité de surveillance vis-à-vis de l'exécutif cantonal et de l'administration qui en dépend et, d'autre part, favorise un choix des membres effectué prioritairement sur la base des compétences requises. Par rapport à la situation actuelle, la composition de la Commission est légèrement modifiée pour inclure également un ou une juriste et un ou une spécialiste en informatique et en sécurité des données (al. 2). Cette composition correspond déjà à celle actuellement en place, même si la loi ne le prévoit pas expressément.
2. Les attributions de la Commission sont énoncées à l'article 50. Il s'agit des fonctions dirigeantes de l'Autorité, qui exigent une légitimation accrue. La Commission remet, en outre, chaque année au Grand Conseil, par l'intermédiaire du Conseil d'Etat, le rapport d'activité de l'Autorité. La faculté qu'elle a d'informer le public de ses constatations, lorsque l'intérêt général le justifie, est une conséquence de son indépendance.
3. Le projet prévoit que la procédure de nomination du ou de la préposé-e est menée par la Commission en collaboration avec la Direction à laquelle l'Autorité est rattachée. C'est toutefois à la Commission que revient la tâche d'émettre le préavis à l'attention du Conseil d'Etat. Ce mode de nomination respecte les exigences du droit supérieur qui laissent aux Etats membres une assez grande latitude de jugement à cet égard. Selon le droit européen, il importe surtout que la procédure de nomination des membres de l'Autorité soit transparente. Celle-ci peut toutefois être conduite tant par le parlement que par le gouvernement, le chef de l'Etat ou un organisme indépendant (cf. comp. art. 43 Directive UE/2016/680 ; 53 RGPD). En Suisse, la nomination du ou de la préposé-e suit plusieurs schémas différents. Dans certains cantons, il ou elle est nommé-e par le parlement sur la

base d'une proposition du Conseil d'Etat (p. ex. : BE ; BL ; GE ; GL ; LU ; SO), d'une commission (AI ; BS) ou directement (VS ; ZH). Dans d'autres cantons, c'est le gouvernement qui nomme le ou la préposé-e (AG ; AR ; GR ; NE et JU ; OW ; SG ; SH ; TI ; UR ; VD ; ZG).

4. Eu égard à la composition de l'Autorité qui compte à la fois une commission spécialisée et un ou une préposé-e, la situation à Fribourg est différente de celle des autres cantons. Puisque la Commission est déjà nommée par le Grand Conseil, il ne paraît pas pertinent de soumettre également à la compétence du Grand Conseil la nomination du ou de la préposé-e qui est l'organe opérationnel de l'Autorité. Dans ce cas, une nomination par le Conseil d'Etat est tout à fait appropriée. D'une part, cette solution correspond à ce que permet le droit européen. D'autre part, c'est aussi la solution appliquée par près de la moitié des cantons en Suisse.
5. En fin de compte, le régime proposé présente de nombreux avantages. Il offre pour la Commission toute la légitimité tirée d'une élection par le Grand Conseil et garantit pour le ou la préposé-e l'intervention d'une autorité indépendante dans le processus de sélection. Ce régime tout à fait unique au sein de l'administration souligne le statut spécial de l'Autorité et de ses membres. Il va largement plus loin que le régime minimal prévu en droit européen. En comparaison intercantonale, il est également tout aussi sinon plus protecteur que la plupart des régimes en place.

### *Art. 51 à 54, Préposé-e*

1. Le ou la préposé-e est l'organe opérationnel de l'Autorité dans le domaine de la protection des données. Afin de lui laisser accomplir ses missions de manière efficace, la loi lui réserve un statut particulier.
2. Selon l'article 51, le ou la préposé-e est nommé-e par le Conseil d'Etat pour une période de cinq ans, reconductible. Le choix d'un engagement pour une période limitée dans le temps s'aligne sur le droit fédéral (cf. art. 44 n-LPD) et le droit européen (cf. art. 44 par. 1 let. e Directive (UE) 2016/680 ; 54 par. 1 let. e RGPD). Il se retrouve également, semble-t-il, à ce jour auprès de l'ensemble des cantons qui ont d'ores et déjà procédé à la révision de leur propre loi. Il est le pendant du régime spécial qui protège le ou la préposé-e durant sa période de fonction. Durant cette période, l'article 52 prévoit que les rapports de travail du ou de la préposé-e ne peuvent être résiliés qu'en cas de faute ou de négligence grave, ou en cas d'incapacité de longue durée (al. 3). La décision de relever le ou la préposé-e de ses fonctions est prise par le Conseil d'Etat de sa propre initiative ou à l'initiative de la Commission. Dans les deux cas, le Conseil d'Etat demande le préavis de la Commission (al. 4). Ce statut unique dans l'administration vise à permettre au ou à la préposé-e d'accomplir ses missions de manière efficace et indépendante. A la fin de la période d'engagement, c'est-à-dire tous les cinq ans, les rapports de travail du ou de la préposé-e à la protection des données sont, en principe, reconduits tacitement (art. 52 al. 1). Le Conseil d'Etat peut néanmoins par voie de décision décider de ne pas reconduire les rapports de travail. Dans ce cas, il doit toutefois solliciter d'abord le préavis de la Commission. La décision de non-reconduction doit parvenir au ou à la préposé-e six mois au moins avant la fin de la période de fonction. Elle doit être suffisamment motivée et elle est susceptible de recours. L'article 53 énonce les règles à suivre en cas d'empêchement de la part du ou de la préposé-e. Tant que le projet ou son ordonnance d'exécution ne prévoient rien de contraire, la législation sur le personnel de l'Etat reste applicable aux rapports de travail du ou de la préposé-e (art. 51 al. 4).
3. La liste des tâches du ou de la préposé-e à la protection des données est énoncée à l'article 54. L'augmentation de cette liste par rapport à la loi actuelle est due, en partie, aux nouvelles tâches dans le domaine de la protection des données, mais aussi, en partie, à la volonté de mieux répartir les tâches entre la Commission et le ou la préposé-e.

### *Art. 55, Autocontrôle de l'Autorité de surveillance*

Cette disposition oblige l'Autorité de surveillance à s'assurer par des mesures de contrôle appropriées portant notamment sur l'organisation et la sécurité des données personnelles du respect et de la bonne application des dispositions de protection des données en son sein.

### 2.5.2 Section 5.2 : Pouvoir de contrôle et d'intervention de l'Autorité de surveillance

#### *Art. 56 à 59, Contrôle par le ou la préposé-e*

1. Conformément aux exigences du droit supérieur, le projet renforce les moyens d'intervention de l'Autorité de surveillance en les alignant sur les nouveaux standards des lois de protection des données.

2. Les moyens d'intervention de l'Autorité de surveillance ont été répartis en deux catégories : ceux qui reviennent directement au ou à la préposé-e et ceux qui sont du ressort de la Commission.

   2.1. Le ou la préposé-e est l'organe compétent pour mener une enquête auprès d'un responsable du traitement ou d'un sous-traitant afin de vérifier qu'il respecte les dispositions de protection des données (art. 56 al. 1). Il ou elle peut le faire d'office ou suite à une dénonciation de la part d'un tiers. Dans le cadre de ses enquêtes, le ou la préposé-e dispose d'un accès illimité à toutes les informations utiles à l'accomplissement de ses tâches ; il ou elle peut en particulier exiger la production de documents, procéder à des auditions ou réaliser une inspection sur place (al. 2). Les obligations de confidentialité ne lui sont pas opposables, sous réserve du secret professionnel (al. 3). Les personnes concernées qui dénoncent une situation problématique à l'Autorité n'ont pas qualité de partie à la procédure. Elles sont toutefois informées des suites données à leur plainte et, sous une forme appropriée, du résultat d'une éventuelle enquête. Dans les cas les plus graves ou persistants, le ou la préposé-e a la possibilité de prononcer une recommandation dans laquelle il ou elle invite le responsable du traitement à se mettre en conformité dans un délai déterminé (art. 57). La recommandation doit alors être suffisamment précise pour comprendre quels sont les reproches formulés et quel type de mesures doivent être prises pour y remédier. Dans le délai imparti, le destinataire rend une détermination sur la suite qu'il entend donner à la recommandation. En cas de refus total ou partiel de la recommandation, le ou la préposé-e peut saisir la Commission.

   2.2. En tant qu'organe collégial élu par le Grand Conseil, la Commission de la transparence, de la protection des données et de la médiation est l'organe compétent pour rendre des décisions contraignantes à l'égard des responsables du traitement (art. 58). Sous réserve des cas de menaces graves et imminentes (al. 3), la Commission ne peut intervenir pour rendre une décision que sur la base d'une saisine du ou de la préposé-e à la protection des données suite à une recommandation infructueuse. La Commission peut ordonner différentes mesures allant de la suspension ou la modification du traitement jusqu'à sa mise à l'arrêt et à la destruction des données déjà collectées. Dans les décisions qu'elle rend, la Commission respecte le principe de proportionnalité. Le ou la préposé-e participe avec voix consultative à la procédure devant la Commission. Il ou elle peut être chargé-e de l'instruction de l'affaire (al. 4). Le fait que le ou la préposé-e ait déjà rendu une recommandation dans la même affaire ne constitue pas un motif de partialité l'empêchant d'instruire l'affaire pour la Commission. A noter que le prononcé d'une recommandation ou d'une décision n'est jamais une fin en soi. Si le responsable du traitement remédie au problème dans le cadre de la procédure devant le ou la préposé-e ou devant la Commission, les deux peuvent classer l'affaire et renoncer à se prononcer (art. 57 al. 5 et 58 al. 5). La Commission a aussi la possibilité de se limiter à un avertissement.

3. L'article 59 rappelle que tant le ou la préposé-e que la Commission respectent, dans leurs interventions, les règles du CPJA. En plus du droit d'être entendu de l'organe visé, qui est expressément mentionné, cela inclut le respect des principes de la légalité, de l'égalité de traitement, de la proportionnalité, de la bonne foi et de l'interdiction de l'arbitraire, le droit à une décision suffisamment motivée ou encore les règles en matière de représentation.

#### *Art. 60, Coopération avec d'autres autorités de protection des données*

La disposition fixe les règles à suivre lorsque l'Autorité de surveillance est amenée à coopérer avec d'autres autorités de protection des données et à échanger dans ce cadre des données personnelles ou, éventuellement, des données soumises à un secret (entraide administrative). En revanche, elle ne concerne pas les différentes formes de

collaboration informelles qui ne portent pas sur des affaires particulières (organisation de manifestations, formations, séminaires, *etc*.).

## 2.6 Section 6, Dispositions transitoires

### *Art. 61, Réglementation d'exécution*

La disposition prévoit une délégation de compétence en faveur du Conseil d'Etat pour qu'il complète le projet sur différents aspects dès lors qu'il existe un besoin pour ce faire.

### *Art. 62, Droit transitoire*

1. Le passage au nouveau droit, notamment le renforcement des exigences en matière de sécurité à l'égard des responsables du traitement, serait difficile sans un temps d'adaptation. Il ne semble pas non plus exigible d'appliquer l'ensemble des nouvelles exigences à tous les traitements sans exception, alors que certains d'entre eux ont débuté à une époque où ce type d'exigences n'avait pas cours. C'est pourquoi le projet prévoit certaines dérogations et introduit des délais pour que les responsables du traitement se mettent en conformité avec le nouveau droit.
2. Un délai général de deux ans est prévu pour permettre aux responsables du traitement de se mettre en conformité avec les nouvelles exigences de la LPrD ; les annonces relatives à une violation de la sécurité des données devront cependant être annoncées à l'Autorité de surveillance ou aux personnes concernées dès l'entrée en vigueur de la loi (al. 1).
3. Tant que la finalité du traitement reste inchangée et qu'il n'y a pas de nouvelles collectes de données qui justifieraient une telle analyse, les obligations relatives à la réalisation d'une analyse d'impact en matière de protection des données ne s'appliquent pas aux traitements qui ont débuté sous l'ancien droit et qui perdurent après l'entrée en vigueur du nouveau droit (al. 2). La réalisation d'une analyse d'impact représente une charge de travail importante. Exiger de l'administration qu'elle rattrape une telle obligation alors que les traitements concernés ont débuté sous l'empire d'autres règles serait déloyal et disproportionné.
4. Une règle spéciale est prévue pour les traitements ayant débuté sous l'ancien droit et qui sont terminés au moment de l'entrée en vigueur de la nouvelle loi (al. 3). Ils continueront d'être soumis aux exigences de la LPrD de 1994. En revanche, dans la mesure où cela est techniquement réalisable, les personnes concernées sont autorisées à invoquer les nouveaux droits prévus à la section 3 de la loi dès l'entrée en vigueur de celle-ci (droit d'accès élargi, droit d'opposition).
5. Pour se mettre en conformité avec la Directive (UE) 2016/680 qui est devenue contraignante pour la Suisse à partir du 1er août 2018 (cf. FF 2017 6565, p. 6783), les responsables de traitement qui entrent dans le champ d'application de la Directive devront tout mettre en œuvre afin de satisfaire dès l'entrée en vigueur de la nouvelle loi au devoir d'informer la personne concernée de la collecte de ses données et aux obligations relatives à la mise en œuvre de la loi prévues à la section 4 du projet (al. 4).

### *Art. 63, Adaptation de la législation*

L'article 5 du projet modifie en partie les exigences sur la manière de rédiger les bases légales en matière de protection des données. L'article 63 octroie un délai de deux ans dès l'entrée en vigueur de la nouvelle loi pour que les Directions procèdent aux éventuelles adaptations de leur portefeuille législatif. Le délai prévu initialement était d'une année. Les retours de la consultation ont toutefois montré que ce délai n'était pas assez long notamment eu égard à la lenteur du processus législatif.

### *Art. 64, Rapports de service du ou de la préposé-e*

Vu la réunification des fonctions de préposé-e à la transparence et de préposé-e à la protection des données (cf. commentaire de l'art. 47) et le passage vers un engagement d'une durée limitée dans le temps (cf. commentaire de l'art. 51), les rapports de service du ou de la préposé-e doivent être adaptés. Même si le passage d'un contrat de durée indéterminée vers un contrat de durée déterminée peut, de prime abord, sembler moins favorable pour la

personne en poste, dans les faits, il n'en résulte pour elle aucune véritable péjoration. Le ou la préposé-e bénéficiera d'une protection renforcée durant toute la durée des rapports de fonction (cinq ans) et retombera tous les cinq ans dans un régime proche de celui applicable à tout employé-e de l'Etat tout en restant plus protecteur. En effet, la décision de ne pas reconduire le mandat du ou de la préposé-e doit être fondée sur de justes motifs et parvenir au ou à la préposé-e six mois avant la fin de son mandat ; elle requiert, en outre, impérativement le préavis de la Commission (cf. art. 52 al. 1). Pour le reste, le Conseil d'Etat veillera à insérer dans la règlementation d'exécution une disposition garantissant le droit au traitement du ou de la préposé-e en cas de maladie ou d'accident survenant durant les rapports de fonction pendant le délai de protection de 730 jours prévu dans la législation sur le personnel de l'Etat (cf. art. 110 al. 4 LPers).

## 2.7 Modification d'autres lois

### 2.7.1 Adaptation de la LStat

Les modifications apportées aux articles 5 al. 1 et 16 al. 2 et 3 ont essentiellement pour but de renvoyer à la nouvelle version de la loi sur la protection des données qui sera adoptée par le Grand Conseil. Le projet propose toutefois, en plus, de corriger une erreur de plume qui s'est glissée à l'article 16 al. 2. Ce n'est pas l'accès aux données qui est interdit mais bien leur publication, lorsqu'elles permettent l'identification ou la déduction d'informations sur la situation individuelle de personnes. Le fait qu'il s'agisse d'une erreur de plume ressort très clairement du Message du Conseil d'Etat du 25 octobre 2005 ayant accompagné le projet de loi sur la statistique cantonale[11].

### 2.7.2 Adaptation de la LOCEA

A la demande de l'ATPrDM et sur le modèle de la Confédération (cf. art. 57h et 57h$^{bis}$ LOGA), le projet propose d'introduire un nouvel article 58a dans la LOCEA permettant aux organes de l'administration de gérer un système de gestion des affaires pouvant contenir des données personnelles, y compris des données sensibles. Cette disposition ne vise pas à remplacer les différentes règles exigées pour le traitement des données dans la législation spéciale mais fournit une base légale pour l'enregistrement et la conservation des données récoltées sur les infrastructures électroniques de l'administration.

### 2.7.3 Adaptation de la LJ

***Art. 46a et 71a***

1. Le projet prévoit l'introduction d'un correspondant ou d'une correspondante à la protection des données auprès du Tribunal cantonal (art. 46a) et du Ministère public (71a).
2. Ces deux entités tombent sous le coup de la Directive (UE) 2016/680 sur la protection des données dans le domaine de la police et de la justice. Cette Directive représente pour la Suisse un développement de l'acquis de Schengen (cf. § 1.3.2.2). Conformément à l'article 32 de la Directive, une personne répondante en matière de protection des données doit être désignée. La personne à désigner doit avoir des connaissances suffisantes de la législation en matière de protection des données et une position assurant que ses prises de position seront respectées. Comme à l'article 45 LPrD, le correspondant ou la correspondante en matière de protection des données doit être en mesure d'exercer ses fonctions de manière autonome. Il ou elle n'est toutefois pas habilité-e à s'immiscer dans une affaire juridictionnelle en cours. La fonction de correspondant ou de correspondante à la protection des données peut être cumulée avec une autre fonction au service des entités concernées.

***Art. 140***

La modification de l'article 140 al. 1 let. b anticipe l'adoption d'une nouvelle législation en matière de sécurité de l'information. La modification de l'article 140 al. 1 let. c relève de la cosmétique législative. Elle aurait, en principe, dû être introduite au moment de l'adoption de la LArch.

[11] BGC 2006 p. 13.

### 2.7.4 Adaptation de la LCo

L'article 102a reprend l'article 58a LOCEA pour les communes.

### 2.7.5 Adaptation du CPJA

***Art. 66a***

Sans pour autant se substituer au pouvoir d'appréciation de l'autorité, des algorithmes peuvent servir parfois comme outil d'aide à la décision dans le cadre d'une procédure. Pour des raisons de transparence et de loyauté, l'article 66a prévoit que le recours à ce type d'outils doit systématiquement être mentionné dans la décision qui est rendue et permet au destinataire de la décision de recevoir une information appropriée sur leur mode de fonctionnement.

***Art. A-4a***

1. Par rapport à l'avant-projet, la disposition sur les décisions individuelles automatisées a été déplacée de la LPrD au CPJA. La raison est qu'il s'agit d'une règle de procédure avant tout. Or, en matière de procédure, le canton est uniquement compétent pour la procédure administrative. Les procédures civiles et pénales sont, en revanche, de la compétence exclusive de la Confédération qui a réglé cette matière de manière exhaustive dans le code de procédure civile du 19 décembre 2008 (CPC ; RS 272) et le code de procédure pénale du 5 octobre 2007 (CPP ; RS 312.0). Une règle de procédure cantonale – même placée dans la LPrD – ne peut par conséquent pas avoir d'effets sur ces deux types de procédure. Comme le Tribunal cantonal exclut à ce stade de recourir à des décisions individuelles automatisées dans le cadre de procédures juridictionnelles et ne voit pas l'utilité d'une telle règle lui étant applicable[12], la disposition a été placée dans l'Annexe I sur la procédure électronique, car cette annexe s'applique uniquement aux autorités administratives de première instance.
2. La particularité des décisions individuelles automatisées est d'être rendues exclusivement sur la base d'un traitement automatisé de données. Il n'y a donc aucun humain qui prend part à l'élaboration de la décision. Les domaines qui se prêtent à ce type de décision restent néanmoins à ce jour encore très limités, car seules des opérations de subsomption très succinctes et rudimentaires peuvent être accomplies par une machine. Il existe malgré tout un certain potentiel dans le domaine de l'administration de masse lorsque des milliers de décisions relativement semblables sont rendues régulièrement sur la base de simples opérations de calcul. A titre d'exemple, les amendes d'ordre pour excès de vitesse pourront certainement un jour être rendues de manière entièrement automatisée. On peut aussi imaginer que certaines autorisations peu complexes pourront être rendues à l'avenir de cette manière.
3. Comme les algorithmes à la base de ces décisions ne sont pas infaillibles et qu'ils peuvent se tromper, il importe de compenser ce risque par des garanties de procédure adaptées. Une décision individuelle prise sur le seul fondement d'un traitement automatisé de données doit obligatoirement être présentée comme telle au moyen d'une mention explicite (al. 1). A la demande du destinataire de la décision, l'administration doit, au surplus, lui communiquer la logique et les critères du traitement ayant généré la décision. Cette garantie est nécessaire pour permettre à la personne concernée d'apprécier le bien-fondé de la décision avant d'éventuellement la contester. Un réexamen extrajudiciaire rapide et gratuit des opérations de traitement liées à une décision automatisée peut être demandé lorsqu'il apparaît de manière claire que celle-ci est entachée d'un vice manifeste et non juridique qui est entièrement imputable à la machine. Sous l'angle procédural, la demande de réexamen suit les mêmes règles qu'en cas de réclamation au sens de l'article 103 CPJA. Toutefois, un réexamen ne peut pas être demandé lorsque l'autorité n'est pas tenue d'entendre une partie avant de rendre sa décision. La règle renvoie à l'article 58 CPJA.

[12] Cf. Prise de position du Tribunal cantonal du 17 mai 2022 en réponse à une question posée.

### 2.7.6 Adaptation de la LVid

L'installation d'un système de surveillance à grande échelle couvrant de grandes parties du domaine public représente une atteinte grave aux droits et aux libertés des personnes concernées. C'est pourquoi elle requiert, entre autres conditions, de procéder à chaque fois à une étude d'impact relative à la protection des données au sens des articles 41 et 42 du projet LPrD (art. 4 al. 3 et 5 al. 1 let. *c*). La loi ne définit pas à partir de quand un système de surveillance couvre de grandes parties du domaine public. La règle est toutefois reprise de l'article 22 al. 2 let. *b* n-LPD, si bien qu'il sera possible de se baser pour répondre à cette question sur les commentaires et la jurisprudence relatifs à cette disposition.

### 2.7.7 Adaptation de la LInf

***Art. 33 et 39***

Les modifications apportées à l'article 33 al. 1 et 2 et 39 sont une conséquence de la réunion des fonctions de préposé-e à la transparence et de préposé-e à la protection des données.

***Art. 40***

La modification de l'alinéa 1 let. b est une conséquence de la réunion des fonctions de préposé-e à la transparence et de préposé-e à la protection des données. C'est aussi le cas de la suppression de l'alinéa 1 let. b$^{bis}$ puisque la question de la nomination et du statut du ou de la préposé-e est déjà réglée dans la LPrD.

***Art. 41***

L'alinéa 1$^{er}$ est supprimé car la question de l'engagement du ou de la préposé-e à la protection des données et à la transparence est réglée dans la LPrD. L'alinéa 2 est adapté en conséquence.

***Art. 42a***

Cf. Commentaire de l'article 64 LPrD.

### 2.7.8 Adaptation de la LMéd

***Art. 5, 6 al. 2 let. b, 8 et 9***

Toujours dans l'objectif d'unifier le régime juridique applicable aux trois membres de l'ATPrDM, les articles 5 et 6 al. 2 let. b sont modifiés et les articles 8 et 9 sont supprimés, car le contenu de ces derniers se retrouve déjà dans la réglementation applicable au ou à la préposé-e à la transparence et à la protection des données.

***Art. 27***

Cf. Commentaire de l'article 64 LPrD.

### 2.7.9 Adaptation de la LCyb

***Art. 30***

Cf. Commentaire de l'article 19 al. 2 et 3 LPrD.

***Art. 35 à 35b***

1. Le passage à la cyberadministration est un processus complexe nécessitant parfois de passer par des phases d'apprentissage avant de retenir définitivement la solution souhaitée[13]. Ces phases d'apprentissage peuvent requérir de déroger momentanément à une règle existante avant de proposer, le cas échéant, son abrogation ou sa modification définitive. Selon la loi actuelle, un projet pilote permet uniquement de déroger à l'obligation de s'appuyer sur une base légale au sens formel pour traiter des données personnelles sensibles. Avec la modification proposée, il sera dorénavant possible de déroger momentanément à d'autres types de normes, lorsque celles-ci contiennent des références à un objet ou à un procédé analogique susceptibles de constituer une entrave à la digitalisation.

—

[13] MONTAVON Michael, *De la planification à la codification de la cyberadministration*, in : RSJ/SJZ 16-17/2022 803-812.

2. La tenue d'un projet pilote est strictement encadrée par des conditions de fond et de forme réparties aux articles 35 à 35b. Sur le fond, un projet pilote doit nécessairement servir à l'accomplissement de tâches publiques ou qui poursuivent un intérêt public avéré, la sécurité des personnes doit être assurée par des mesures appropriées et il doit exister un besoin d'expérimentation reconnu justifiant la tenue d'un projet pilote avant l'adoption des bases légales définitives. Sur la forme, un projet pilote doit suivre un protocole clairement établi composé de plusieurs étapes. Sa durée ne devrait, en principe, pas excéder cinq ans et il nécessite impérativement la préparation préalable d'un dossier complet, un rapport d'évaluation à la fin de la phase pilote et l'intervention de différents acteurs aux différentes étapes de son déroulement. Surtout, un projet pilote doit être prévu au moyen d'une ordonnance (expérimentale) dont la durée et le champ d'application sont limités afin d'assurer une publicité et un encadrement suffisants au projet. Ce n'est qu'à l'issue du projet pilote qu'un projet de loi sera, le cas échéant, finalement soumis au Grand Conseil. L'avantage de ce procédé est qu'il permet d'augmenter la sécurité et la précision de la loi, car les normes proposées ont pu être élaborées de manière empirique plutôt que sur la base uniquement d'hypothèses. Leur qualité s'en trouve renforcée.
3. L'article 35 al. 3 contient un renvoi exprès vers l'article 22 LPrD qui traite des projets pilotes portant sur le traitement de données sensibles, la conduite d'activités de profilage ou d'autres types de traitements susceptibles de présenter un risque élevé pour les droits des personnes concernées. Il s'agit alors de coordonner les deux dispositions. Pour cette catégorie de projets, on applique les règles générales de la LCyb applicables à tous les projets pilotes et les règles supplémentaires de la LPrD applicables aux projets pilotes portant sur des traitements de données particuliers. Concrètement, ces règles supplémentaires portent sur l'implication de l'ATPrDM aux différentes étapes du projet.
4. L'administration recourt parfois à des tiers pour l'accomplissement de certaines tâches. Cela peut aussi être le cas en matière de cyberadministration où des partenariats public-privé peuvent constituer des solutions adaptées. Or, selon l'article 54 Cst. cant., toute délégation de tâches publiques à des tiers requiert d'être prévue dans une loi. Dans l'hypothèse où la tenue d'un projet pilote impliquerait le recours à un tiers, l'article 35b al. 2 constituerait alors la base légale requise durant toute la durée du projet pilote mais pas au-delà (al. 1).
5. Selon l'article 35b al. 2, la possibilité de mener un essai pilote est étendue aux communes dans leurs domaines de compétence.

### 2.7.10 Adaptation de la LS

L'article 43 al. 3a constitue la base légale pour la transmission de certaines données relatives aux élèves, au corps enseignant et au personnel administratif à la Fédération des services d'identité de l'espace suisse de formation (Edulog) afin de pouvoir accéder notamment à des moyens d'enseignement en ligne. Edulog utilise le NAVS 13 uniquement pour fédérer et défédérer une identité. Un identificateur technique est attribué de manière aléatoire et le NAVS n'est jamais enregistré.

La modification de l'article 43 al. 4 a pour seul but de renvoyer à la nouvelle version de la loi qui sera adoptée par le Grand Conseil.

### 2.7.11 Adaptation de la LESS

Même commentaire que pour la LS s'agissant de la modification de l'article 43.

### 2.7.12 Adaptation de la LFE

Le progiciel SAP (ci-après : le système de gestion intégré) est utilisé par les services et établissements de l'Etat depuis de nombreuses années. La gestion financière et la comptabilité sont en principe réalisées au moyen de cet outil mis à disposition des diverses unités administratives par l'Administration des finances. L'utilisation de ce système donne entière satisfaction. Pour satisfaire aux exigences de la protection des données (nécessité d'une base légale formelle), le présent projet ancre l'utilisation d'un tel progiciel dans la législation sur les finances de l'Etat.

### *Section 6a*

Il est prévu d'insérer les dispositions régissant le système de gestion intégré des finances de l'Etat dans une nouvelle subdivision de la LFE, numérotée 6a, et suivant les dispositions d'organisation. Les trois articles composant cette subdivision énoncent les dispositions de base requises par la législation sur la protection des données. Ces articles précisent quelles sont les catégories de données traitées et la finalité du traitement des données. Ils décrivent en outre le fonctionnement et les modalités d'accès au système de gestion intégré. Le projet de loi renvoie aux dispositions d'exécution s'agissant de la répartition des responsabilités et des mesures de sécurité à mettre en place.

### *Art. 47a*

1. Cette disposition décrit les finalités de l'utilisation du système de gestion intégré par les services et établissements de l'Etat, ainsi que le contenu de ce système d'information.
2. Les finalités sont énoncées à l'alinéa 1. Il s'agit de la gestion financière et opérationnelle, ainsi que de la planification financière et du suivi budgétaire.
3. L'énoncé des buts poursuivis par l'utilisation du système de gestion intégré est exhaustif et correspond à la pratique actuelle. L'utilisation du mot « notamment » dans le projet de loi vise simplement à ne pas alourdir inutilement la procédure dans l'hypothèse, peu probable, où la liste devrait être complétée, à l'avenir, par une opération nouvelle connexe, non envisagée actuellement.
4. L'alinéa 2 fixe pour sa part les catégories de données traitées par le truchement du système de gestion intégré. Il s'agit des éléments suivants :
   a) identités et adresses des personnes physiques et des personnes morales qui ont des relations financières avec l'Etat ;
   b) informations sur les coordonnées financières des personnes visées par la lettre a) et sur leurs transactions financières avec l'Etat.
5. L'identité des personnes physiques englobe les informations relatives à leurs noms, prénoms, adresses, données de contact, dates de naissance et, le cas échéant, de décès, nationalité, lieu d'origine, sexe, langue de correspondance, coordonnées bancaires (IBAN), numéro AVS, numéro d'identifiant cantonal de personne (ICP) et autres identifiants nécessaires à la gestion financière du dossier de la personne concernée (Symic [numéro utilisé dans le domaine de la migration], PID Gelan [Identifiant des exploitations agricoles du système de gestion des exploitations agricoles et des paiements directs], No RegEdu [numéro utilisé dans le domaine de l'éducation], etc.
6. L'identité des personnes morales comprend quant à elle les données sur la raison sociale, le statut juridique, l'adresse, les données de contact, la date de création et, le cas échéant, celle de liquidation, la langue de correspondance, les coordonnées bancaires (IBAN), les numéros TVA, IDE (identifiant des entreprises suisse), REE (registre des entreprises et établissements) et ICP, ainsi que les autres identifiants nécessaires à la gestion financière du dossier de la personne morale concernée.
7. Ici également, l'utilisation du mot « notamment » dans le projet de loi vise simplement à ne pas alourdir inutilement la procédure si, par hypothèse, il devait être nécessaire de compléter à l'avenir la liste des catégories de données traitées. A l'heure actuelle, seules les données des deux catégories visées par le projet sont traitées dans le système de gestion intégré.
8. Conformément au droit de la protection des données, il est mentionné à l'alinéa 3 que des données sensibles peuvent être traitées au moyen du système de gestion intégré des finances. Certains établissements et services de l'Etat qui utilisent ce logiciel pour leur facturation sont actifs dans des domaines « sensibles » au sens du droit de la protection des données, ainsi les domaines de la police, de l'action sociale, etc. L'alinéa 3 donne une assise légale formelle à ces traitements de données. A cet égard, il est important de noter que les mesures techniques et organisationnelles pour garantir la sécurité des traitements sont d'ores et déjà prises. En effet, le système est

construit « en silo », de sorte que chaque utilisateur ou utilisatrice n'ait accès qu'aux données qui le ou la concernent et dont il ou elle a besoin pour l'exercice de ses tâches. A cet égard, l'alinéa 3 précise que le traitement de données sensibles par le truchement du système de gestion intégré n'est autorisé que si l'accomplissement des tâches « financières », telles que précisées à l'alinéa 1, en dépend.

### *Art. 47b*

1. L'alinéa 1 précise quels sont les organes utilisateurs du système de gestion intégré. Il s'agit principalement des unités administratives de l'Etat, soit les établissements et les services. Ces entités ont la possibilité, mais pas l'obligation, d'utiliser le système de gestion intégré. En pratique, seules quelques unités sont autorisées à ne pas utiliser ce système pour leur comptabilité. Il s'agit par exemple des hautes écoles et des universités. En ce qui concerne les communes, elles peuvent avoir accès au système de gestion intégré dans la mesure où elles doivent pouvoir consulter leur compte courant par le biais de Platcom (plateforme de communication entre l'Etat et les communes). Il est important de noter que les communes ont uniquement accès aux données qui les concernent directement en lien avec leur gestion financière et comptable.
2. Les alinéas 2 et 3 précisent les flux de données : les établissements et services utilisent le système de gestion intégré pour leur comptabilité et facturation ainsi que pour les opérations liées à la planification financière et à la procédure budgétaire. L'Administration des finances peut accéder, dans le cadre des attributions qui lui sont conférées par la législation sur les finances de l'Etat (encaissement des factures et gestion du contentieux/planification financière et procédure budgétaire), à l'ensemble des données contenues dans le logiciel. Des mesures particulières sont prises s'agissant des services traitant des données personnelles particulièrement sensibles.
3. Conformément aux exigences du droit de la protection des données, l'alinéa 4 ancre dans la loi la possibilité d'interfacer le système de gestion intégré avec d'autres systèmes d'information. Il n'est pas souhaitable d'énumérer et fixer dans la loi les systèmes concernés. En effet, le domaine est particulièrement évolutif et il ne serait pas efficient de devoir modifier la LFE lors de chaque nouvel interfaçage ou de chaque suppression d'un interfaçage existant. Cela dit, pour écarter les risques d'abus, l'alinéa 4 est formulé de manière restrictive. Les interfaçages doivent respecter le principe de finalité prévu par la législation sur la protection des données et ne peuvent être réalisés qu'en lien avec la gestion financière et la comptabilité de l'Etat.
4. Le système de gestion intégré des finances est déjà actuellement interfacé avec d'autres systèmes d'information, tels que le système de gestion de l'éducation (HAE), egov ou encore e-kogu (système utilisé dans le domaine des hospitalisations hors canton). Il sera prochainement interfacé avec le Référentiel cantonal selon la procédure et les modalités prévues par les dispositions régissant le Référentiel cantonal.
5. L'alinéa 5 prescrit que l'accès aux données du système de gestion intégré par procédure d'appel est autorisé. Ce type d'accès est soumis aux règles spéciales du droit de la protection des données : il doit ainsi être formalisé par un règlement d'utilisation qui précise les personnes autorisées à accéder aux données, les données mises à leur disposition, la fréquence des interrogations, la procédure d'authentification, les autres mesures de sécurité ainsi que les mesures de contrôle (art. 21 al. 3 du règlement du 29 juin 1999 sur la sécurité des données personnelles ; RSF 17.15). Comme pour l'interfaçage, la finalité du traitement doit être conforme à la législation sur les finances de l'Etat.
6. L'alinéa 6 règle la communication à d'autres autorités ou à des tiers. Ces traitements de données répondent aux mêmes exigences que l'interfaçage et la procédure d'appel. Ils ne sont autorisés que dans un but conforme à la législation sur les finances de l'Etat. Les cas envisagés sont par exemple la transmission aux communes des données relatives à la perception des émoluments du registre foncier, pour leur permettre le prélèvement des centimes additionnels, ou des données nécessaires à la perception de l'impôt sur les chiens. Les utilisateurs et utilisatrices ne sauraient en aucun cas s'appuyer sur cette disposition pour transmettre à des tiers des données dans un but sans lien avec la gestion financière et la comptabilité de l'Etat.

***Art. 47c***

1. Pour tenir compte du caractère évolutif du domaine de la sécurité informatique, le projet de loi délègue au Conseil d'Etat la compétence de fixer les mesures de sécurité, d'ordre organisationnel et techniques, qui devront être prises pour garantir la sécurité des données en lien avec l'utilisation du système de gestion intégré.
2. Comme déjà indiqué, le système de gestion intégré est mis à disposition des établissements et services de l'Etat par l'Administration des finances. De nombreuses entités sont ainsi appelées à utiliser cet instrument. Il importe que les responsabilités des divers intervenants soient clairement établies. Dès lors qu'il s'agit en l'espèce d'une question essentiellement organisationnelle, le projet prévoit également de déléguer au Conseil d'Etat la tâche de répartir les responsabilités entre les diverses entités concernées.
3. Le projet précise néanmoins que le détail des mesures de sécurité à mettre en œuvre ainsi que celui de la répartition des responsabilités peut faire l'objet de conventions passées entre l'Administration des finances et les entités utilisatrices du système de gestion intégré et que, le cas échéant, les conventions doivent être transmises à l'Autorité cantonale de la transparence, de la protection des données et de la médiation pour assurer sa bonne information.

#### 2.7.13 Adaptation de la LSan

Selon la modification apportée à l'article 60 al. 3 LSan, le droit d'accéder à ses données personnelles dans le domaine de la santé ne pourra plus être conditionné à la présence d'un ou d'une professionnel-le de la santé, ce mode de consultation pouvant uniquement être proposé à la personne concernée. Ce changement va dans le sens d'un meilleur respect de l'autonomie de la personne concernée et de son droit à l'autodétermination informationnelle.

# 3 Liste des principales abréviations

—

## 3.1 Actes législatifs

Ancienne Directive (UE) 95/46/CE : Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 24 octobre 1995

ap-LPrD : avant-projet de révision de la loi cantonale sur la protection des données du 27 novembre 2019

Convention STE 108 : Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (RS 0.235.1)

Convention STE 108+ : Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel des 17 et 18 mai 2018

CPC : Code de procédure civile suisse du 19 décembre 2008 (RS 272)

Cst. cant. : Constitution du canton de Fribourg du 16 mai 2004

CPJA : Code de procédure et de juridiction administrative du canton de Fribourg du 23 mai 1991 (CPJA ; RSF 150.1)

CPP : Code de procédure pénale suisse du 5 octobre 2007 (RS 312.0)

Décision-cadre 2008/977/JAI : Décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale du 27 novembre 2008 (journal officiel de l'Union européenne (L 350/60)

Directive (UE) 2016/680 : Directive (UE) 2016/680 du 27 avril 2017 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales,

d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales et abrogeant la décision-cadre 2008/977/JAI du Conseil

LArch : Loi du 10 septembre 2015 sur l'archivage et les Archives de l'Etat (RSF 17.6)

LBCF : Loi du 22 novembre 1988 sur la Banque cantonale de Fribourg

LCH : Loi du 23 mai 1986 sur le contrôle des habitants (RSF 114.21.1)

LCo : Loi du 25 septembre 1980 sur les communes (RSF 140.1)

LCyb : Loi du 18 décembre 2020 sur la cyberadministration (RSF 184.1)

LEE : Loi concernant les rapports entre les Eglises et l'Etat (RSF 190.1)

LFE : Loi du 25 novembre 1994 sur les finances de l'Etat (RSF 610.1)

LInf : Loi du 9 septembre 2009 sur l'information et l'accès aux documents (RSF 17.5)

LJ : Loi du 31 mai 2010 sur la justice (RSF 130.1)

LMéd : Loi du 25 juin 2015 sur la médiation administrative (RSF 181.1)

LOCEA : Loi du 16 octobre 2001 sur l'organisation du Conseil d'Etat et de l'administration (RSF 122.0.1)

LOGA : Loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (RS 172.010)

LPD : Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1)

LPD, 1ère modification : Modification du 24 mars 2006 de la loi fédérale sur la protection des données (RO 2007 4983)

LPD, 2e modification : Loi fédérale portant mise en œuvre de la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (RO 2010 3387)

LPers : Loi du 17 octobre 2001 sur le personnel de l'Etat (RSF 122.70.1)

LPrD : Loi du 25 novembre 1994 sur la protection des données (RSF 17.1)

LResp : Loi cantonale sur la responsabilité civile des collectivités publiques et de leurs agents (RSF 16.1)

LS : Loi du 9 septembre 2014 sur la scolarité obligatoire (RSF 411.0.1)

LESS : Loi du 11 décembre 2018 sur l'enseignement secondaire supérieur (RSF 412.0.1)

LSan : Loi du 16 novembre 1999 sur la santé (RSF 821.0.1)

LSF : Loi fédérale du 9 octobre 1992 sur la statistique fédérale (RS 431.01)

LSR : Loi fédérale du 16 décembre 2005 sur l'agrément et la surveillance des réviseurs (RS 221.302)

LStat : Loi du 7 février 2006 sur la statistique cantonale (RSF 110.1)

LTN : Loi fédérale du 17 juin 2005 concernant des mesures en matière de lutte contre le travail au noir (RSF 822.41)

LTrans : Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (RS 152.3)

LVid : Loi du 7 décembre 2012 sur la vidéosurveillance (RSF 17.3)

n-LPD : Nouvelle loi fédérale du 25 septembre 2020 sur la protection des données (FF 2020 7397 ; entrée en vigueur prévue en septembre 2023)

RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

RSI : Règlement sur la sécurité de l'information (en cours de préparation)

## 3.2 Autres abréviations

al. : alinéa

art. : article

ATF : Arrêt du Tribunal fédéral

AVS : Assurance-vieillesse et survivants

BGC : Bulletin officiel des séances du Grand Conseil

ch : chiffre

CHF : franc suisse

cf. : confer

comp. : comparaison

consid. : considérant

éd. : édition

EPT : équivalent plein temps

FF : Feuille fédérale

JAAC : Jurisprudence des autorités administratives de la Confédération

let. : lettre

NAVS : Numéro d'assurance vieillesse et survivants

Par. : paragraphe

RO : Recueil officiel fédéral

ROF : Recueil officiel fribourgeois

RSB : Recueil systématique bernois

RSDA : Revue suisse de droit des affaires et du marché financier

RSF : Recueil systématique de la législation fribourgeoise

RSJ : Revue suisse de jurisprudence

UE : Union Européenne