RAPPORT EXPLICATIF

accompagnant l'avant-projet de loi sur la révision totale de la loi sur la protection des données

En bref

1. La loi actuelle sur la protection des données 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 25 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'autres part, à améliorer la sécurité des infrastructures, des processus et de l'organisation qui soutiennent ces traitements. La Confédération et la plupart des cantons procèdent ainsi actuellement eux aussi à la révision de leur législation en matière de protection des données en vue d'atteindre ces objectifs.

4. L'avant-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 le projet actuel de révision totale de la loi fédérale sur la protection des données, lequel a lui-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 ainsi que les nouvelles exigences du droit de l'Union européenne en matière de protection des données. Il reprend aussi l'une ou l'autre disposition intéressante que d'autres cantons ont intégrée dans leur propre législation et dont les **effets positifs** ont été reconnus par la doctrine.

5. Quand bien même le projet de révision de la loi fédérale sur la protection des données a exercé une influence importante sur la réalisation du présent avant-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 de projets actuellement en cours relatifs à la digitalisation de l'administration. On peut citer à titre d'exemple les éléments suivants :

— des règles particulières sont prévues dans le but de permettre **une externalisation sûre et contrôlée** de certaines formes de traitement auprès de prestataires tiers, lorsque ceux-ci disposent de compétences et de ressources spécifiques et pointues que les services spécialisés de l'Etat ne sont pas en mesure de fournir eux-mêmes ;

— pour respecter la **composition bipartite de l'Autorité cantonale de la transparence** et de la protection des données, les nouveaux pouvoirs qui sont accordés à l'autorité de surveillance en matière de protection des données 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 et de la protection des données ;

— contrairement au projet de révision de la loi fédérale sur la protection des données, l'avant-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 l'avant-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 de traitements visent de manière générale à aligner la loi fribourgeoise sur **les nouveaux standards applicables** en matière de protection des données à l'ère de la digitalisation. La mise en œuvre de ces standards est une condition nécessaire de la réussite et du succès de la stratégie cantonale de cyberadministration dans la mesure où il ne peut y avoir de digitalisation sans confiance numérique.

7. Le plan du présent rapport est le suivant :

1 généralités 3
1.1 Contexte et origine de l'avant-projet 3
1.2 Déroulement des travaux 5
1.3 Grandes lignes de l'avant-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 9
1.3.3 Droit des personnes concernées 10
1.3.4 Obligation des responsables du traitement 11
1.3.5 Autorités de surveillance en matière de protection des données 12
1.4 Conséquence de l'avant-projet 13
1.5 Conformité au droit supérieur 15
2 Commentaire des dispositions 15

2.1 Section 1, dispositions générales 15
Art. 1, But 15
Art. 2, Champ d'application personnel 15
Art. 3, Champ d'application matériel 16
Art. 4, Définitions 18
2.2 Section 2, Principes régissant le traitement de données personnelles 20
2.2.1 Section 2.1, Conditions *générales de licéité du traitement* 20
2.2.2 Section 2.2 : Conditions supplémentaires applicables à certaines formes de traitement 23
2.2.3 Section 2.3 : Traitement de données à des fins ne se rapportant pas à la personne 28
2.3 Chap. 3, Droits des personnes concernées 29
2.4 Chap. 4, Mise en œuvre de la protection des données 32
2.5 Chap. 5, Surveillance 38
2.5.1 Section 5.1 : Autorités de surveillance en matière de protection des données 38
2.5.2 Section 5.2 : Pouvoir de contrôle et d'intervention de l'autorité de surveillance 41
2.5.3 Section 5.3 : Autres tâches de l'autorité de surveillance 44
2.6 Chap. 6, Dispositions transitoires 44
2.7 Adaptation de la législation spéciale 45
2.7.1 Adaptation de la LStat 45
2.7.2 Adaptation de la LJ 45
2.7.3 Adaptation de la LVid 45
2.7.4 Adaptation de la LGCyb 46
2.7.5 Adaptation de la LInf 46
2.7.6 Adaptation de la LS 46
2.7.7 Adaptation de la LPol 46
2.7.8 Adaptation de la LSan 47

Les lois et règlements cités le sont avec leurs abréviations ; une liste de celles-ci figure à la fin du document.

1 GENERALITES

1.1 Contexte et origine de l'avant-projet

1.1.1. En matière de protection des données, **plusieurs générations de législations** se sont succédées 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 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 (dite « Convention STE 108 »), elle est caractérisée par une approche fondée sur **des grands principes** (licéité, proportionnalité, finalité, 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 la Directive 95/46/CE 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 qui est promulguée en 1995. En Suisse, la Confédération adopte en 1992 la LPD. 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 précisés et/ou 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 surveillance. 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 du Conseil de l'Union européenne relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. 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 en tenant compte de certains développements intervenus ; 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 strictement le droit supérieur. Mais d'autres cantons vont plus loin et procèdent à des améliorations plus substantielles de leur loi en matière de protection des données.

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+. 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 leur 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. De son côté, le Conseil fédéral a jugé qu'il était nécessaire de procéder à la révision totale de la LPD et a proposé à cette fin un projet de loi accompagné d'un Message en septembre 2017. En septembre 2018, le Parlement fédéral a adopté la LPDS qui introduit un premier lot de modification visant à permettre à la Suisse de se conformer aux exigences du droit européen dans le cadre des accords de Schengen-Dublin dans les délais fixés.

1.1.2. Adoptée en 1994, la LPrD n'a été modifiée sous l'angle matériel **qu'une seule fois** en 2008. A l'origine, le projet de révision comptait trois volets (Cf. 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.

1.1.3. 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* ».

1.1.4. Autrement dit, la LPrD se situe aujourd'hui **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 qui non seulement offre aux citoyens et aux citoyennes une protection adaptée et cohérente en matière de protection des données, mais qui réponde aussi aux exigences et aux standards internationaux qui lient la Suisse dans ce domaine.

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 la Préposée à la protection des données 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'imposen**t 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 la Préposée comprend un représentant de chacune des Directions, un représentant du pouvoir judiciaire, un représentant du Ministère public, un représentant de la Police, deux représentants du Service de l'informatique et des télécommunications, un représentant des communes ainsi qu'un représentant du Service de

législation. Pour permettre d'avancer de manière efficace dans les travaux de révision, le groupe de travail a décidé de constituer un groupe de travail restreint composé de la Préposée à la protection des données et du représentant du Service de législation, qui a été chargé de rédiger les dispositions légales et de les soumettre pour discussion aux membres du groupe de travail complet. En cours de travaux, d'autres **sous-groupes de travail** ont été constitués pour discuter de thématiques plus spécifiques avec les acteurs principalement concernés notamment dans le domaine de la police et de la technique.

1.2.3. Le groupe de travail complet a porté des efforts importants sur la recherche d'**un juste équilibre** entre deux objectifs parfois opposés : d'une part les **impératifs du droit de la protection des données** et la nécessité de s'aligner autant que possible sur les nouveaux standards de la troisième génération de législation dans ce domaine et, d'autre part,la nécessité pour les organes publics de disposer d'une **marge de manœuvre suffisante** pour pouvoir exécuter avec succès et sans entrave inutile les tâches que la Constitution et les lois leur confient.. Certaines dispositions proposées initialement par le groupe de travail restreint, très focalisées sur le premier objectif, ont dans cette perspective été retravaillées pour atteindre également le deuxième objectif. Au final, le résultat proposé permet ainsi de satisfaire **dans toute la mesure du possible** tant aux exigences du droit de la protection des données qu'à celles relatives au bon fonctionnement de l'administration.

1.3 Grandes lignes de l'avant-projet

1.3.1 Contenu en général

1.3.1.1. Le contenu général de l'avant-projet ressort clairement de **sa structure** qui reste pratiquement inchangée par rapport à la loi actuelle. Comme cette dernière, il comporte six sections : la première contient les traditionnelles dispositions générales et une série de définitions qui servent à donner un sens précis à des termes qu'on retrouve plusieurs fois dans l'avant-projet (art. 1 à 4) ; la deuxième section fixe les principes généraux qui régissent le traitement des données personnelles et les règles plus précises qui concernent certains types de traitement particuliers (art. 5 à 25) ; la troisième section énonce les droits dont disposent les personnes concernées lorsque leurs données personnelles sont traitées art. 26 à 36) ; la quatrième section décrit les mesures que les responsables de traitement doivent respecter et mettre en œuvre lorsqu'ils traitent des données personnelles afin d'assurer leur protection et leur sécurité (art. 36 à 47) ; la cinquième section traite de la surveillance exercée par l'autorité de contrôle en matière de protection des données (art. 49 à 64) et la sixième section contient les habituelles dispositions de droit transitoire qui indiquent comment les nouvelles règles qui seront adoptées s'insèreront dans le droit existant (art. 65).

1.3.1.2. Le contenu des dispositions proposées **s'inspire en grande partie** du projet du Conseil fédéral sur la révision totale de la LPD, lequel est lui-même inspiré par les nouveaux textes de la troisième génération de législation en matière de protection des données que

représentent la Convention STE 108+, le Règlement (UE) 679/2016 et la Directive (UE) 680/2016. Ces réglementations ont influencé le contenu de l'avant-projet principalement à trois niveaux :

a) L'avant-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 que pour ceux dont les activités sont moins risquées (cf. FF 2017 6565, p. 6593).

b) L'avant-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. 20). 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 équivaloir à ignorer cette dernière, sous peine que la loi ne n'atteigne pas ses objectifs.

c) La **terminologie employée** dans l'avant-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 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.

1.3.1.3. A l'instar du projet du Conseil fédéral et contrairement au droit de l'Union européenne, l'avant-projet **renonce à mentionner** expressément l'existence d'un « ***droit à l'oubli*** » (cf. art. 17 Règlement (UE) 2016/679) de même qu'à introduire un droit généralisé à la « ***portabilité des données*** » (cf. art. 20 Règlement (UE) 2016/680) pour les raisons suivantes :

a) La formulation « droit à l'oubli » est trompeuse car elle laisse entendre à tort la consécration d'un droit général pour les personnes concernées de disparaître des bases de données de l'Etat. Or un tel droit ne peut bien évidemment pas être reconnu. L'avant-projet prévoit en revanche d'autres garanties **plus circonstanciées** qui peuvent en pratique aboutir à la reconnaissance d'un droit à l'oubli (dans le même sens : FF 2017 6565, p. 66693). Il s'agit, d'une part, de l'article 10 qui prévoit que les données personnelles qui ne sont plus nécessaires au regard des finalités du traitement doivent d'office être supprimées (ou anonymisées) et, d'autre part, de l'article 30 al. 2 let. a qui permet à la personne concernée de demander elle-même l'effacement de ses données lorsqu'elles ne présentent plus d'utilité. En outre, l'article 33 autorise la personne concernée à demander la suppression de certaines données la concernant après sa mort.

b) Le droit à la portabilité des données permet à la personne concernée de récupérer ses données personnelles en vue de leur réutilisation pour un usage personnel ou dans le but de les transférer à un organisme tiers. Il implique par conséquent une transmission dans un

format structuré, couramment utilisé et en principe facilement lisible par n'importe quelle machine. Cela suppose une standardisation et une normalisation des supports et des logiciels informatiques utilisés par les administrations des communes, des cantons et de la Confédération, voire même des Etats étrangers si on considère le droit à la portabilité des données du point de vue européen. Avant d'introduire un droit généralisé à la portabilité des données dans le canton de Fribourg, il semble ainsi **opportun d'attendre** les résultats et les développements de la Stratégie « Suisse numérique », ainsi que des expériences au sein de l'Union européenne dans ce domaine (dans le même sens : FF 2017 6565, p. 6607).

1.3.1.4. En comparaison avec le projet du Conseil fédéral, l'avant-projet compte 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]. Le Tribunal fédéral n'a pour sa part pas clairement tranché la question[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 final 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 du p-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

[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 ; AUER/ MALINVERNI / HOTTELIER, *Droit constitutionnel suisse, vol. II*, 3e éd., Berne 2013, n° 384 ; 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] Dans l'ATF 137 II 371, le Tribunal fédéral a déclaré que les personnes morales bénéficient de la protection de la sphère privée qui comprend aussi la protection des données personnelles. Il a ajouté qu'elles ne seraient néanmoins pas titulaires de tous les aspects protégés par l'art. 13 Cst. sans pour autant donner plus d'indications à ce sujet (consid. 6).

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 le p-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 l'avant-projet.

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 règlement général (UE) 2016/679 sur la protection des données, 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 aux domaines de la justice et de la police. La Directive (UE) 2016/680 n'étant pas directement applicable ni pour les Etat 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 certaines 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 règlement général (UE) 2016/679 (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 de traitements 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 Règlement (UE) 2016/679). 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 **intenable** 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 procèdera prochainement à une nouvelle évaluation du droit suisse afin de vérifier sa compatibilité avec le Règlement général (UE) 2016/679. Dans le cadre de cette évaluation, elle examinera le droit fédéral mais aussi le droit de certains cantons choisis 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. Entrée en vigueur le 1er octobre 1985, 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 des 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 Règlement (UE) 2016/679 et la Directive (UE) 2016/680, la Convention STE 108+ a un contenu très semblable à ces deux textes. Le Conseil fédéral **a d'ores et déjà signé** le Protocole d'amendement à la Convention le 30 octobre 2019. Il sera prochainement soumis au Parlement fédéral en vue de son approbation.

1.3.3 Droit des personnes concernées

1.3.2.1. La question des droits des personnes concernées est traitée au chapitre 3 de l'avant-projet. L'un des buts de l'avant-projet est de **renforcer le contrôle et la maîtrise** des personnes concernées sur les informations qu'elles partagent avec les collectivités publiques. Il introduit dans ce but de nouveaux droits mieux adaptés aux évolutions des usages numériques et facilite les conditions et les modalités de leur exercice.

1.3.2.2. De nouveaux droits sont introduits, en particulier :
a) La faculté pour toute personne de pouvoir s'opposer préventivement à la communication de données déterminées la concernant à des tiers (**droit de blocage**). 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 de blocage appartient en Europe et en Suisse de longue date 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 29 de l'avant-projet. Le droit de blocage 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 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 l'utilisation de certaines de ses données tout en permettant au responsable du traitement de continuer de pouvoir les conserver (art. 33 al. 1 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, alors que des vérifications sont nécessaires pour vérifier le bien-fondé de la demande.
c) Des moyens de défenses spécifiques et adaptés sont reconnus à l'article 31 de l'avant-projet en faveur des personnes faisant l'objet d'une **décision fondée exclusivement sur un traitement automatisé de données** (par exemple, au moyen d'un algorithme). Dans ce cas, la personne concernée doit toujours être informée qu'il s'agit d'une décision rendue exclusivement par une machine. Elle a aussi le droit de demander de connaître la logique et les critères à la base de celle-ci, et, le cas échéant, de demander qu'elle soit revue par une personne humaine.

d) Une nouvelle disposition est proposée à l'article 33 qui accorde à toute personne la faculté de décider du sort de ses données personnelles **après sa mort** dans un cadre délimité.

1.3.2.3. 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 illicite de ses données.

1.3.4 Obligation des responsables du traitement

1.3.4.1. Les obligations du responsable du traitement de données sont définies au chapitre 4 de l'avant-projet. Il fixe les mesures d'organisation et de sécurité encadrant le traitement de données personnelles par les organes publics et les responsabilités y relative.

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. 37). Comme c'est le cas déjà actuellement, cette responsabilité est assurée et mise en œuvre de manière **transparente et systématique** : tout traitement de données à l'intérieur de l'Etat est placé sous la responsabilité d'un responsable de traitement, qui est tenu de déclarer celui-ci dans le registre des activités de traitement (art. 38 à 40) et d'assurer la protection et la sécurité des données par des mesures concrètes qui sont adaptées aux circonstances (art. 41).

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 citées expressément. La première signifie que des mesures techniques et organisationnelles adaptées doivent être discutées et mises en place dès les premières étapes de la conception des opérations de traitement afin de préserver le plus tôt possible les droits et les libertés des personnes concernées (art. 42 al. 1). 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 (art. 42 al. 2).
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 de traitement est tenu d'accomplir préalablement u**ne analyse d'impact relative à la protection des données** (art. 43). Le but de cette analyse d'impact est double : il vise, d'une part, à aider les responsables du traitement à construire des traitements de données respectueux de la vie privée et, d'autre part, à démontrer leur conformité à la loi sur la protection des données ;

c) En cas de violation de la protection des données, le responsable du traitement doit **annoncer la violation** dans les plus brefs délais à l'Autorité cantonale de la transparence et de la protection des données et, dans les cas les plus graves, directement à de la personne concernée (art. 45 et 46).
d) Les organes publics qui traitent des données personnelles sur une base régulière systématique doivent nommer **un correspondant ou une correspondante en matière de protection des données** (art. 47). Cette personne a pour rôle d'accompagner sous l'angle juridique les responsables du traitement dans le déroulement de leurs activités et de faire le lien, lorsque cela est nécessaire, avec l'Autorité cantonale de la transparence et de la protection des données. Le correspondant ou la correspondante en matière de protection des données n'assume en revanche **aucune responsabilité personnelle** par rapport aux activités de traitement qu'il ou elle accompagne.

1.3.5 Autorités 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 disposent **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 qui ne respecteraient 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. Lorsque l'organe public refuse d'y donner suite, l'autorité de surveillance a néanmoins la possibilité de porter l'affaire en justice (cf. art. 22a LPrD).

1.3.5.2 L'avant-projet **renforce la position** de l'autorité de surveillance. Il s'agit là d'une obligation claire 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 en matière de protection des données en Europe, de la Confédération et des autres cantons, l'Autorité cantonale de la transparence et de la protection des données doit disposer non seulement de pouvoir d'investigation mais aussi **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, l'avant-projet prévoit que le ou la préposé-e a la protection des données n'aura qu'un **pouvoir d'injonction** lui permettant de demander au responsable du traitement qui ne respecterait pas entièrement ses obligations de prendre les mesures nécessaires en vue de respecter la loi (art. 58). La compétence de prononcer **une décision contraignante** en matière de protection des données revient au final à la Commission cantonale de la transparence et de la protection des données (art. 59). Cette dernière est un **organe pluridisciplinaire** élu par le Grand Conseil qui est composée en particulier d'un-e juriste, d'un professionnel ou d'une professionnelle de la santé, d'un ou d'une spécialiste des

technologies de l'information et de la communication et d'un professionnel ou une professionnelle des médias.

1.4 Conséquence de l'avant-projet

a) Changements dans la pratique administrative

1.4.1 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 Règlement (UE) 2016/679 et de la Directive (UE) 2016/680, **un véritable bouleversement** des pratiques administratives semble néanmoins **peu probable**.

1.4.2 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 25 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 disposent généralement déjà de ressources techniques et en personnel supplémentaires dédiées à cette fin.

b) Conséquences financières et en personnel

1.4.3 Dans la mesure où l'avant-projet procède pour l'essentiel à une **adaptation à du droit supérieur** qui est de toute manière obligatoire, il n'entraîne pas, de par lui-même, de conséquences financières et en personnel directes. Mais il est vrai que pour se conformer aux nouvelles exigences de l'avant-projet les différents organes de l'Etat devront ponctuellement **puiser dans leurs ressources disponibles**, notamment lorsqu'il s'agira d'accomplir une étude d'impact relative à la protection des données ou d'assurer le suivi d'un incident en matière de protection des données. En outre, la formalisation au niveau de la loi de la fonction de **correspondant-e en matière de protection** des données impliquera pour les unités administratives concernées de trouver en leur sein les ressources nécessaires à l'accomplissement de cette tâche.

1.4.4 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 (cf. les projets de

Référentiels cantonaux transverses). La révision de la loi, associée à la mise en œuvre de la stratégie Fribourg 4.0, générera inévitablement **de nouvelles exigences techniques**, notamment en matière de traçabilité des données. 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 tout à fait normal **d'y associer la protection des données**. Pour faire face à une éventuelle augmentation des demandes de traçabilité, il sera nécessaire dans certains domaines d'automatiser les processus afin d'alléger les traitements manuels et pour se conformer aux exigences de délais imposées par la loi. 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 (journalisation d'évènements, journalisation des connexions, historisation de la consommation de données etc.) 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, qu'il est difficile de chiffrer à ce stade.

1.4.5 Comme l'a relevé le Conseil fédéral dans son Message concernant la révision totale de la LPD (cf. FF 2017 6565, p. 6783), c'est surtout dans le domaine de la surveillance que les changements apportés auront un impact marqué. Car l'avant-projet introduit toute une série de **nouvelles tâches** pour l'ATPrD comme pour le ou la préposé-e à la protection des données. Ces nouvelles tâches viennent s'ajouter à **la charge de travail supplémentaire** à laquelle l'Autorité doit déjà faire face depuis plusieurs années dans le cadre de la digitalisation de l'Etat à laquelle elle participe étroitement soit directement en prenant part à plusieurs groupes de travail sur différents projets dans ce domaine, soit indirectement au travers des nombreux conseils qu'elle rend dans ce domaine ainsi que dans le cadre des consultations législatives. Or, depuis sa création en 1994, les ressources en personnel de l'ATPrD consacrées à la protection des données n'ont été augmentées qu'une seule fois en 2009 par l'octroi de 0,5 EPT pour un poste de juriste. Ce nouveau poste est venu s'ajouter à celui de de Préposé-e à la protection des données qui passera, lui, de 0,5 à 0,8 EPT à partir du 1er janvier 2020. A ce jour, l'Autorité connaît **une surcharge de travail chronique** qui non seulement rend extrêmement difficile l'accomplissement de ses tâches au quotidien, mais qui conduit aussi parfois à retarder la réalisation de certains projets informatiques d'importance. C'est pourquoi une augmentation des **ressources en personnel de l'ATPrD** est à ce stade inévitable. Le besoin exact en ressources fera l'objet d'une analyse plus précise en collaboration avec le Service du personnel et d'organisation dans le cadre de la mise en œuvre de la loi.

Notons à cet égard que l'octroi de ressources suffisantes à l'Autorité de surveillance constitue un élément important tant au niveau de la décision d'adéquation et de la mise en œuvre des acquis de Schengen que de la ratification par la Suisse de la Convention STE 108+

(art. 42, par. 4 de la directive (UE) 2016/680 ; art. 52 par. 4 du Règlement (UE) 2016/680 et art. 15 par. 6 de la Convention STE 108 modernisée).

1.5 Conformité au droit supérieur

L'avant-projet est compatible avec la Constitution cantonale, le droit fédéral et aussi les obligations internationales de la Suisse. Il fait 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 modernisée.

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, l'avant-projet indique que la loi vise à garantir les ***droits fondamentaux*** des personnes concernées, sans préciser lesquels.

Art. 2, Champ d'application personnel

1. Le champ d'application personnel de l'avant-projet est pour l'essentiel calqué sur celui de la loi actuelle :
a) Il recouvre tout d'abord l'ensemble des organes qui relèvent des **autorités législatives, exécutives et judiciaires** aux échelons cantonal, communal et intercommunal, y compris les établissements de droit public (personnalisés ou non) et les corporations de droit public cantonal (p. ex., syndicats de remaniement des terrains à bâtir, syndicats d'amélioration foncière, sociétés de droit public fondées sous la forme d'une société anonyme ou d'une société coopérative), auxquels il faut également ajouter des organismes particuliers comme la Banque cantonale ou le Conseil de la magistrature.
b) Il recouvre aussi 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. Les particuliers qui accomplissent des tâches de droit public sont par exemples les notaires et les médecins engagés dans des

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

hôpitaux publics. Parmi les institutions visées, on peut citer l'Union fribourgeoise du tourisme ou la Société des cafetiers, restaurateurs et hôteliers s'agissant de la formation des futurs exploitants.
c) Conformément à l'article 3 al. 2 LEE, **les paroisses et les autres corporations ecclésiastiques** sont des corporations de droit public. Pour cette raison, elles entrent en principe dans le champ d'application actuel de la loi. L'avant-projet réserve toutefois la possibilité pour les Eglises d'adopter leurs propres dispositions en la matière et d'instituer leur propre autorité de surveillance (cf. art. 2 al. 1 let. c et 48 al. 3). En pareil cas, l'autorité cantonale de surveillance en matière de protection des données continuera d'exercer la **haute surveillance** sur l'autorité ecclésiastique de surveillance en matière de protection des données.

2. En plus des cas visés à l'alinéa 1er, l'avant-projet introduit à l'alinéa 2 la possibilité pour l'autorité cantonale de surveillance en matière de protection des données d'agir **auprès d'autres institutions situées sur le territoire cantonal** dans le cadre d'un accord de collaboration avec le Préposé fédéral à la protection des données (le PFPDT) ou avec une autre autorité de surveillance en matière de protection des données. Par exemple, le PFPDT pourrait en cas de soupçon de violation des dispositions de protection des données par une entreprise du canton de Fribourg demander à l'autorité cantonale d'aller enquêter sur place, en particulier lorsque l'entreprise en question entretient des rapports étroits avec l'Etat ou une commune. La plus grande proximité de l'autorité cantonale et sa meilleure connaissance du terrain devrait dans ce cas faciliter les échanges et les possibilités de trouver des solutions. A noter que le **renforcement de la collaboration** entre les autorités de surveillance en matière de protection des données constitue un des objectifs de la révision globale du droit de la protection des données (cf. art. 60 ss du Règlement (UE) 2016/679 ; art. 50 de la Directive (UE) 2026/680 et art. 17 de la Convention STE 108+).

Art. 3, Champ d'application matériel

1. En droit interne, la protection des données est régie de **manière générale** par une loi-cadre sur la protection des données et de **manière spéciale** par différentes réglementations sectorielles qui servent à régler certaines situations de manière spécifique. Par définition, la réglementation spéciale ne réglemente pas la question de la protection des données **de manière exhaustive** dans le domaine qu'elle traite mais uniquement **à titre accessoire**.

2. Pour **éviter la survenance de lacunes** en matière de protection des données, l'avant-projet prévoit que la loi est dans chaque cas au minimum applicable **en complément** à la législation spéciale (al. 2). Cela signifie que les réglementations spéciales pourront continuer de compléter les règles générales, voire de déroger à celles-ci, dans les domaines qu'elles traitent mais que la réglementation générale restera toujours applicable aux situations et aux questions qui ne sont pas traitées par la législation spéciale. La règle est inspirée du § 3 al. 3 de la loi cantonale de Bâle-Ville sur l'information et la protection des données du 9 juin 2010 (Gesetz über die Information un den Datenschutz [IDG] ; 153.260).

3. Conséquence de ce changement, l'avant-projet ne prévoit **plus d'exception fixe** au champ d'application matériel de la loi (comparaison : art. 2 al. 2 LPrD). Il en résulte notamment que :
a) 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) tombe. Pareille exception était motivée autrefois par le **principe du secret** qui prévalait à l'intérieur de l'Etat. Or ce principe a depuis largement été battu en brèche notamment avec l'adoption en 2009 de la loi sur l'information et l'accès aux documents (LInf ; RSF 17.5), 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 ; NE et JU ; OW ; NW ; GL et BE). Sa suppression semble de ce fait parfaitement viable pour les organes visés. 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.
b) L'exception fixe concernant **les procédures** civiles, pénales et de juridiction administrative en cours (art. 2 al. 2 let. b) est remplacée par deux exceptions **mieux ciblées** qui auront pour effet à la fois d'assurer le fonctionnement correct de la justice et aussi la protection des droits des personnes concernées dans ce domaine également. La première exception a pour but **d'empêcher l'application concurrente** des dispositions de la loi sur la protection des données avec les garanties de procédure énoncées dans les codes de procédure ; elle prévoit que les droits et les prétentions des personnes concernées dans le cadre de procédures en cours sont régis exclusivement par le droit de procédure applicable (art. 32). La deuxième exception est introduite dans le but de garantir **l'indépendance de la justice** ; elle déclare que l'autorité de surveillance en matière de protection des données n'est **pas compétente** pour contrôler la bonne application de la loi à l'égard des traitements de données effectués par des organes publics dans l'exercice de leurs fonctions juridictionnelles (art. 62).

4. Pour ne pas créer de distorsion en matière de concurrence, l'alinéa 3, à l'instar de la loi actuelle (art. 2 al. let. c LPrD), prévoit que les dispositions cantonales en matière de protection des données ne sont pas applicables aux organes publics lorsqu'ils mènent des activités **en situation de concurrence économique** et qu'ils n'agissent pas en qualité d'organe investi de la puissance publique. Contrairement à la loi actuelle, l'avant-projet prévoit néanmoins que la surveillance reste dans ce cas du ressort de l'autorité cantonale de surveillance en matière de protection des données et non du Préposé fédéral. Ce faisant, on **évite** qu'un seul et même organe ne soit soumis simultanément à la surveillance de deux **autorités différentes** en matière de protection des données. On retrouve la même règle

[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.

notamment à l'article 4 al. 2 let. a, 2e phr. de la loi cantonale bernoise du 19 février 1986 sur la protection des données (LCPD ; RSB 152.05).

Art. 4, Définitions

La plupart des définitions contenues dans cet article sont **reprises textuellement ou presque** du projet de révision totale de la loi fédérale sur la protection des données. 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 :
a) En comparaison avec le projet de révision de la loi fédérale, l'avant-projet introduit en plus la notion d'« ***identifiant commun de personne*** » (let. d). Il s'agit d'une sorte de super-donnée qui réunit un ensemble d'attributs personnels propres à une personne permettant une représentation souvent complexe et fine de cette dernière. Une étude récente réalisée sur mandat de l'Office fédéral de la Justice (OFJ) et du PFPDT a démontré qu'en l'absence de mesures de protection adéquates l'utilisation de ces identifiants peut engendrer des **risques réels** pour les droits des personnes concernées. En effet, ils permettent de relier facilement entre elles les données conservées dans différents registres, offrant ainsi aux personnes indélicates ou à des pirates informatiques les moyens d'établir plus rapidement et plus aisément un profil détaillé des personnes concernées[5]. Ce risque grandit au fur et à mesure de l'augmentation du nombre d'organismes ayant recours au même identifiant, notamment parce que les standards de sécurité appliqués peuvent varier entre les différents organes qui l'utilisent (administration cantonale, communale, école, hôpitaux etc.). C'est pourquoi l'avant-projet soumet la création de ces identifiants au respect de règles particulières (art. 5 al. 1). Comme cela ressort de la définition donnée, ces règles trouvent cependant application uniquement à l'égard des identifiants communs de personnes qui sont **partagés entre plusieurs institutions** (tel l'identificateur cantonal de personne au sens de l'art. 14 LGCyb). Cette précision vise à exclure les identifiants sectoriels propres à un organe qui servent à classer plus facilement les personnes avec lesquelles cet organe est en contact. La définition proposée est une adaptation de l'article 4 let. i de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles du canton de Genève (LIPAD ; RSG A 2 08).
b) Même si la définition actuelle de ce que signifie un « ***traitement de données*** » est exemplative et qu'elle est volontairement **très large** pour couvrir toute opération portant sur des données personnelles, elle a été complétée avec les notions ***d'interconnexion*** et ***d'externalisation*** (let. e). Au vu de l'ampleur que ce type de traitement gagne dans la société de l'information, il semble important de rappeler qu'il s'agit de traitements de données **à part entière,** soumis aux exigences fixées dans la loi. Par interconnexion de données, on entend l'opération consistant à créer des informations nouvelles en croisant entre elles des

[5] BASIN David, *Risk Analysis on Different Usages of the Swiss AHV Number – Evaluation on behalf of the Federal Office of Justice and the Federal Data Protection and Information Commissioner*, Zurich 2017. Document consultable à l'adresse : https://www.bj.admin.ch/bj/fr/home/publiservice/publikationen/externe/2017-09-27.html.

données existantes provenant de sources distinctes (pour un exemple fribourgeois, voir l'art. 137 al. 3 LICD). Quant à l'externalisation, la notion fait référence au fait de faire appel à un tiers pour traiter ou héberger des données. Elle recouvre en particulier le recours à des solutions de ***cloud computing***. A l'inverse, l'avant-projet renonce à conserver la définition de ce qu'est **une communication** de données. Dans la mesure où il ne s'agit que d'un type de traitement parmi d'autres, Il n'y a pas véritablement de raison de maintenir cette définition qu'on ne retrouve du reste ni dans la Convention STE 108+, ni dans le droit de l'UE.

c) A l'instar du projet du Conseil fédéral (art. 4 ch. 4 p-LPD) et conformément aux exigences du droit de l'UE (art. 3 par. 4 de la Directive (UE) 2016/680 et art. 4 par. 4 du Règlement (UE) 2016/679), l'avant-projet introduit la notion de **profilage**. Il s'agit d'un nouveau type de traitement considéré comme particulièrement intrusif. Il consiste à mettre volontairement en évidence ou à prédire certaines caractéristiques personnelles essentielles d'un individu, 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**.

d) A l'instar du projet du Conseil fédéral et de la Convention STE 10+, l'avant-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 registre des fichiers qu'on trouve actuellement à l'article 21 LPrD est renommé dans l'avant-projet « registre des activités de traitement » (art. 40) et le « responsable du fichier » mentionné à l'art. 4 let. g de la loi LPrD devient, dans l'avant –projet, « responsable du traitement » (4 let. g). Globalement, ces changements restent néanmoins avant tout d'ordre t**erminologique** et ne devraient pas avoir d'incidence pratique particulière.

e) L'avant-projet renonce à reprendre la définition de ce qu'est une « ***violation de la sécurité des données*** » telle qu'elle figure dans le projet du Conseil fédéral (art. 22 p-LPD) et dans le droit de l'UE (art. 3 ch. 12 de la Directive (UE) 2016/680 et art. 4 ch. 11 du Règlement (UE) 2016/679). Vu son contenu, une telle définition légale est **superflue**. Son caractère vague et général fait qu'elle n'apporte aucune précision utile allant plus loin que son acceptation ordinaire. Dans ce contexte, il semble préférable de laisser à la jurisprudence et à la doctrine le soin de préciser éventuellement cette notion dans la pratique.

f) 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*** ». 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 de 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.

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**. C'est ainsi qu'en principe seule une base légale autorise un organe à traiter des données personnelles.

2. 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.

3. S'alignant sur la pratique de la Confédération et de la totalité des autres cantons en Suisse, l'avant-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 (donnée sensibles, profilage, procédures d'appel, création d'identifiants communs de personnes etc.). Ce type de traitement n'est licite que si une loi au sens formel l'autorise expressément (base légale directe) ou s'il est indispensable à l'accomplissement d'une tâche clairement définie dans une loi au sens formel (base légale indirecte).

4. Vu la pratique de l'Autorité de surveillance, qui a jusqu'ici toujours mis en garde sur la nécessité d'avoir une base légale au sens formel pour ces types de traitement même en l'absence d'une telle exigence explicite dans la loi et la bonne acceptation de cette pratique au sein des administrations, ce changement ne devrait pas avoir une influence pratique considérable. Il exigera néanmoins de vérifier que les traitements en cours sont en adéquation avec la règle.

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 domaines 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 certaines fins. Pour être valable, le consentement doit être **éclairé, libre et explicite** (al. 1). 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 ne se retrouve pas non

plus contrainte de donner son consentement à un traitement qui n'est pas prévu par la loi. Le consentement doit en outre impérativement être accompagné d'un acte positif de la personne concernée, ce qui exclut la possibilité d'un consentement « *par défaut* ». La preuve de l'existence du consentement revient au responsable du traitement qui doit de ce fait consigner l'acte par lequel la personne a consenti à un traitement de données particulier.

2. A noter cependant que la portée du consentement est cependant en principe **moindre en droit public** qu'en droit privé. Dans les relations entre l'administration et les administrés, le fait justificatif principal reste en effet avant tout celui de la légalité du traitement[6]. La collecte, par un organe public, de données qui ne sont pas requises par la loi devrait pour cette raison en principe être réservée à des cas spécifiques et justifiés. De plus, l'administré devrait dans toute la mesure du possible toujours disposer **d'une alternative** au consentement et ne pas se voir pénaliser en cas de refus de donner celui-ci. C'est pourquoi l'avant-projet précise que toute sollicitation du consentement au traitement de données qui n'est pas prévu par la loi doit s'accompagner d'une mention claire et visible de son **caractère facultatif** (al. 2).

Art. 7, Finalité

1. Le principe de finalité présente trois volets (al. 1) :
a) premièrement, il implique que des données personnelles ne peuvent être collectées et traitées que dans un but **préalablement défini**, c'est-à-dire qui n'est ni vague, ni imprécis, ni indéterminé (**principe de détermination**) ;
b) deuxièmement, il exige que le but et les méthodes du traitement, ainsi que les catégories de données traitées, soient globalement **reconnaissables** pour les personnes concernées selon les règles de la **bonne foi** ;
c) finalement, les traitements prévus doivent poursuivre une finalité **légitime**, ce qui exclut les traitement arbitraires qui ne reposent pas sur des motifs sérieux et objectifs et qui n'ont ni sens ni but. Il s'agit ici d'une concrétisation du principe constitutionnel de **l'interdiction de l'arbitraire** en droit de la protection des données.

2. Le principe de finalité entretient un lien étroit avec le pouvoir reconnu à la personne de **maîtriser** les informations la concernant. Dès lors, la personne concernée peut faire usage de ce pouvoir en consentant à une utilisation de ces données à de nouvelles fins. Cette possibilité présentera un intérêt particulier dans le cadre de la mise en œuvre de la stratégie cantonale de **cyberadministration**, qui prévoit la possibilité pour les administrés de décider d'utiliser leurs données afin de bénéficier de services à la carte.

[6] FASNACHT Tobias, *Die Einwillung im Datenschutzrecht : Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwillung im schweizerischen Recht*, thèse Fribourg, Zurich/ Bâle/ Genève 20017, p. 91.

Art. 8, Proportionnalité

1. Elément essentiel du droit de la protection des données, le principe de proportionnalité s'impose lors de **chaque étape** du traitement de données depuis la phase de la collecte jusqu'à leur suppression ou leur archivage. Il concerne non seulement **les données**, mais aussi **le choix des moyens** et des **méthodes** de traitement.

2. Le principe de proportionnalité implique que les données traitées et les méthodes de traitements ne doivent **pas être excessives** par rapport au but du traitement. Cela signifie d'une part que seules peuvent être traitées les données qui sont objectivement nécessaires en vue d'atteindre le but fixé (**principe de minimisation des données)**. Conformément à cette règle, il n'est pas autorisé de traiter des données personnelles qui ne sont pas pertinentes pour le but du traitement (par exemple, le numéro AVS s'agissant de la location d'une place de parc). D'autre part, les méthodes de traitement choisies doivent être **le moins invasif et le moins attentatoire possibles** aux droits des personnes concernées.

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 en toutes circonstances **conformes à la réalité**. 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 la collecte des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées (ou anonymisées). Cela implique pour les responsables du traitement de vérifier à intervalle régulière que les données en leur possession sont toujours pertinentes par rapport aux buts visés. Compte tenu des évolutions technologiques et des capacités presque illimitées de stockage existantes, l'avant-projet fait de cette règle un principe de licéité du traitement.

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. Sont réservées également les règles en matière d'archivage (cf. art. 22 de l'avant-projet).

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 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** appropriées à la situation.

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

Art. 12 à 14, Collecte de données

1. La collecte des données est la phase qui précède directement l'enregistrement des données dans un registre de l'administration. Les données ainsi récoltées sont par la suite **conservées** pour une période plus ou moins longue et peuvent être utilisées dans le cadre de vérifications, de communications ou de décisions. Le **simple fait de collecter des données** à caractère personnel et de les conserver constitue déjà une **ingérence** dans la vie privée des personnes sans égard au fait que les données collectées sont ou non utilisées par la suite[7]. C'est pourquoi toute collecte de données par un organe de l'Etat doit à la fois être r**econnaissable** pour la personne concernée et reposer à chaque fois sur **une base légale ou un autre motif justificatif** prévu par la loi (art. 12 al. 1).

2. Pour s'assurer de la qualité des données récoltées, mais aussi pour permettre à la personne concernée d'exercer ses droits y relatifs, il importe qu'elle soit le plus possible **associée** au processus de collecte des données. L'avant-projet maintient dans ce sens la règle voulant que la collecte de données devrait avoir lieu dans toute la mesure du possible **directement** auprès de la personne concernée. Il ne s'agit néanmoins pas là d'une règle absolue. Un certain nombre de données sont dorénavant mises à disposition des collectivités publiques *via* d'autres moyens, notamment des interfaçages de bases de données et des procédures d'appel (cf. art. 15 al. 2 de l'avant-projet). Dans ce genre de cas, l'absence de participation de la personne concernée est généralement compensée en partie par l'adoption de bases légales appropriées.

3. Dans le but d'améliorer la **transparence** et la **reconnaissabilité** des traitements, l'avant-projet introduit en plus une obligation pour les auteurs de traitements **d'informer les personnes concernées** de la collecte (art. 13). Ce principe constitue aujourd'hui **un standard unanimement reconnu** en matière de protection des données qu'on retrouve déjà dans la version actuelle de la loi fédérale sur la protection des données (art. 18 et 18a LPD) et qui a

[7] ATF 143 I 253, consid. 3.2.

été reprise dans le projet du Conseil fédéral (art. 17 p-LPD). Elle figure également dans le droit de l'UE (art. 13 de la Directive (UE) 2016/680 et art. 13 et 14 du Règlement (UE) 2016/679, ainsi que l'art. 8 de la Convention STE 10+). Les informations à fournir doivent permettre à la personne concernée de comprendre rapidement qui traite des données à son sujet, y compris les sous-traitants, 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. Il n'est pas précisé **la forme** que doit revêtir l'information. 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. 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.

4. Le devoir d'information n'est **pas absolu** : le responsable du traitement peut être dispensé de son devoir d'information si la personne concernée a déjà été informée ou s'il collecte les données auprès d'un tiers et que la collecte est prévue par la loi ou si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés (art. 14 al. 1). Le devoir d'information peut également être **limité ou retardé** aux mêmes conditions que celles prévues en matière de droit d'accès (al. 2).

Art. 15 à 19, 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 de données personnelles. Les **conditions de licéité** ne sont cependant pas les mêmes selon que l'on se trouve dans l'un ou l'autre cas (art. 15 al. 1) :
a) 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 de l'avant-projet ;
b) Les communications uniques de données qui ont lieu **dans un cas d'espèce** n'ont pas besoin d'être prévues au moyen d'une disposition légale mais elles doivent satisfaire à l'une des conditions énumérées à l'article 15, al. 1, let. a à c.

2. L'avant-projet règlemente une troisième catégorie de communication de données : les **communications par voie d'appel** (art. 15 al. 2). Comme c'est le cas actuellement (art. 10 al. 2 LPrD), ce type de communication nécessite l'adoption d'une base légale *ad hoc*. Sur ce point, l'avant-projet s'écarte du projet du Conseil fédéral de révision de la LPD qui propose de supprimer cette exigence se trouvant actuellement à l'article 19 al. 3 LPD. Selon le Conseil fédéral, les exigences liées aux communications par voie d'appel doivent être abandonnées, car elles seraient **dépassées** à l'ère de la société numérique (FF 2016 6565, p. 6698). Cet avis semble toutefois **ne pas pouvoir être suivi**. Une communication par voie d'appel constitue

un mode d'accès automatisé 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 qu'il a reçue. Autrement dit, il s'agit d'un type de traitement qui réunit simultanément les caractéristiques d'une collecte et d'une communication de données selon le principe du **libre-service**. Dans ce contexte, il paraît justifié de prévoir la mise en place de **garde-fous** pour des raisons à la fois de transparence, de gouvernance et de sécurité.

3. Conformément au droit de l'UE (art. 45 ss du Règlement (UE) 2016/679) et de la Convention STE 108+ (art. 14), des exigences supplémentaires s'appliquent en cas de communication de données **à l'étranger** dans le but notamment d'assurer la **libre circulation des données** entre les Etats parties (art. 16) :
a) Selon la règle de base dans ce domaine (art. 16 al. 1), les transferts de données personnelles vers des Etats tiers ne sont en principe autorisés que pour autant que l'Etat destinataire offre un **niveau de protection adéquat**. Pour savoir si un Etat offre ou non un niveau de protection adéquat, il sera possible se référer à **la liste** tenue et mise à jour par le Conseil fédéral conformément à l'article 13 al. 1 p-LPD. A noter que même si elle a vocation à être régulièrement actualisée, le contenu de cette liste peut néanmoins ne **pas être toujours exhaustif**. Aussi l'absence d'un Etat tiers sur cette liste ne signifie pas forcément qu'il n'offre pas un niveau de protection adéquat, mais, le cas échéant, qu'il n'a pas encore fait l'objet d'une évaluation par le Conseil fédéral (cf. FF 2017 6565, p. 6658).
b) Lorsque le pays destinataire 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). La liste des garanties et des motifs justificatifs permettant de palier à l'absence d'une législation suffisante reste **globalement inchangée** par rapport au droit actuel et n'appelle pas de commentaires particuliers.

3.1 Comme en matière de collecte de données (cf. art. 13 de l'avant-projet), l'article 16 al. 3 introduit le devoir pour le responsable du traitement qui communique des données à l'étranger d'en **informer la personne concernée**.

3.2 L'avant-projet prévoit que 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. 16 al. 4) quand bien même ces informations peuvent aussi être consultées à l'étranger. Cette règle se justifie afin d'éviter l'application de règles **disproportionnées** à des situations qui n'en ont pas le 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.

3.3 Conformément à ce que prévoient les articles 49 al. 1 du Règlement (UE) 2016/679 et 12 § 5 et 6 de la Convention STE 108+, l'avant-projet attribue des compétences particulières à l'autorité de surveillance en matière de protection des données en lien avec les flux

transfrontières de données. D'abord, il soumet les responsables du traitement au **devoir d'informer** l'autorité de surveillance des communications de données transfrontières à destination d'un Etat dont la législation n'assure pas un niveau de protection adéquat. Ensuite, il octroie à cette dernière un **pouvoir d'intervention** lorsque les droits des personnes concernées sont insuffisamment protégés (art. 17). Les compétences de l'autorité de surveillance sont décrites aux articles 56 ss de l'avant-projet.

4. Les **restrictions** à la communication de données personnelles formulées à l'article 18 de l'avant-projet restent globalement **inchangées** par rapport à la loi actuelle (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 restriction 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 19 de l'avant-projet **réserve** expressément certaines règles provenant d'autres législations qui peuvent **déroger en partie** aux règles de la loi sur la protection des données.

Art. 20, Externalisation

1. Dans le domaine des systèmes d'information, l'externalisation de certains services auprès de prestataires tiers est devenue **une pratique incontournable** aussi bien pour les entreprises du secteur privé que pour les administrations publiques. Les entreprises du secteur des technologies de l'information et de la communication disposent en effet de ressources et de compétences **hautement spécialisées** qu'aucune autre organisation ne sera jamais en mesure d'égaler aussi bien sous l'angle de la qualité des prestations, de la performance, de la capacité d'innovation ou encore de la sécurité.

2. Le projet pilote mené par le SITel concernant l'externalisation de certaines données dans le *cloud*[8] a déjà permis d'explorer les possibilités techniques dans ce domaine et aussi d'approfondir les aspects sécuritaires afin de s'assurer de l'adéquation de ce type de solution avec les exigences légales en matière de protection des données. Le rapport d'évaluation du SITel a conclu que les retours d'évaluation étaient suffisamment probants pour envisager l'adoption des bases légales nécessaires en vue d'étendre les possibilités de recours à d'autres solutions de *cloud computing*. Tenant compte des enseignements retirés lors de la phase pilote, la présente disposition fait en sorte d'autoriser le recours à ce type de solutions dans un cadre délimité et sécurisé correspondant aux standards les plus élevés dans ce domaine. A noter que cette ouverture correspond à l'un des objectifs du Catalogue de mesures pour **la stratégie d'informatique en nuages** des autorités suisses 2012-2020 (Orientation O2 : Adaptation des bases légales).

3. Des exigences particulières sont fixées pour permettre à la fois aux organes publics de **conserver la maîtrise** des données externalisées et aussi **de garantir la protection** des droits

[8] Cf. l'ordonnance du 4 décembre 2018 autorisant le Service de l'informatique et des télécommunications à externaliser le traitement de certaines données dans le « Cloud » (projet pilote) (RSF 17.41).

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

4. A noter que ces exigences, auxquelles s'ajoutent celles de l'article 18 de l'avant-projet (traitement sur mandat), **reprennent largement** les recommandations de la Conférence des préposé(e)s suisses à la protection des données en matière d'externalisation[9].

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

Art. 21, Essais pilotes

1. Cet article qui est inspiré de l'art. 17a LPD (et qui a été repris à l'art. 31 p-LPD) figure actuellement sous une forme similaire à l'article 21 LGCyb. Un essai pilote au cours duquel des données personnelles sont manipulées représente **un traitement de données** au sens de la législation sur la protection des données. C'est pourquoi l'avant-projet choisit de déplacer cette norme dans la LPrD.

2. La mise en œuvre d'essais pilotes est soumise à des **conditions de fond** qui sont décrites au premier alinéa. La première d'entre elles est que seuls sont autorisés les essais servant l'accomplissement **d'une tâche publique**, qui poursuivent un **intérêt public manifeste** ou encore qui s'inscrivent dans le cadre **d'une stratégie menée par plusieurs administrations en Suisse** conjointement (let. a). Ensuite, **les risques** pour les citoyens doivent être **réduits** autant que possible (let. b). Outre la prise de mesures techniques et organisationnelles, le Conseil d'Etat peut, par exemple, limiter l'essai à une partie du territoire, à certains organes, à certaines dates et à certains objets. Finalement, il est rappelé qu'un essai pilote donne à l'administration la possibilité **de tester et d'examiner** un système avant de créer et de mettre en place le cadre légal nécessaire à son exploitation définitive. Elle n'a en revanche

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

pas pour fonction de permettre d'utiliser un système définitif avant même de disposer des bases légales indispensables (let. c).

3. Selon l'article 54 al. 1 Cst., les organes des collectivités publiques peuvent déléguer l'accomplissement de tâches publiques à des tiers pour autant que la délégation soit prévue au moyen d'une base légale au sens formel. Dans l'hypothèse où la tenue d'un essai pilote implique de confier la réalisation de telles tâches à un prestataire de services externe, l'article 21 al. 4 fait office de base légale nécessaire à la délégation pour la durée de l'essai.

Art. 22, Archivage

Les organes publics gèrent l'archivage des données personnelles conformément à la LArch. Les données personnelles qui ne présentent pas de valeur archivistiques sont en principe supprimées.

Art. 23, Effacement et destruction de données

1. L'article 10 de l'avant-projet fait de l'obligation de détruire les données devenues inutiles une condition de licéité du traitement. La présente disposition indique **la manière** dont cette obligation doit être mise en œuvre.

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 et qui n'ont plus d'utilité doivent être effacées régulièrement (al. 1). 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 (généralement le disque dur) devra être physiquement détruit (al. 2).

Art. 24, Vidéosurveillance

Pas de commentaire.

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

Art. 25, 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 ce genre de traitements sont sensiblement **moins risqués** 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 Chap. 3, Droits des personnes concernées

Art. 26 à 28, Droit d'accès

1. Le droit d'accès (art. 26) 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 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. g. Le fait que celui-ci confie le traitement à un tiers ne change rien à cet égard (al. 3).

2. En tant que pilier du droit de la protection des données, le droit d'accès appartient à toute personne concernée 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 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. 27 al. 1). Pour les demandes d'accès à **des données médicales**, le responsable du traitement (en principe le médecin traitant) 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 (cf. art. art. 60 al. 3 LSan).

3. Le droit d'accès n'est **pas absolu**. L'article 28 de l'avant-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** après avoir procédé à une pesée des intérêts en présence et conformément au principe de proportionnalité.

Art. 29, 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. 21 Règlement (UE) 2016/679 ; art. 9 § 1 let. d Convention STE 108+ ; art. 20 LPD et art. 33 p-LPD).

2. Au niveau des cantons, seul le canton d'Uri ne reconnaît pas un tel droit. Les cantons d'Argovie et de Fribourg limitent pour leur part cette possibilité aux seules données du contrôle des habitants (art. 18 LCH et § 16 de la Gesetz über die Information der Öffentlichkeit, den Datenschutz et das Archivwesen du canton d'Argovie du 24 octobre 2006 [IDAG ; 150.700]). Tous les autres cantons prévoient un droit de blocage général sans égard

au type de données concernées[10]. 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). L'avant-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). 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 est susceptible de sensiblement entraver l'organe public dans l'accomplissement de ces tâches (let. b) ou qu'il aurait pour conséquence d'empêcher une tierce personne de défendre ses intérêts légitimes (let. c). Dans les cas prévus aux lettres b et c, la restriction au droit d'opposition nécessite à chaque fois de procéder à une **pesée des intérêts en présence**. Dans la mesure du possible, la personne concernée sera entendue (al. 3).

Art. 30, actions défensives

1. L'alinéa 1er énonce les trois **moyens défensifs traditionnels** pouvant être invoqués en cas d'atteinte ou de risque d'atteinte aux droits des personnes imputable à un traitement illicite de données. Par rapport au texte actuel de la loi, la phrase introductive a été modifiée pour mieux mettre en évidence que les droits prévus par cette disposition peuvent être invoqués non seulement par la personne concernée, mais également par toute autre personne ou entité ayant un intérêt digne de protection. Outre la personne concernée elle-même qui aura toujours un intérêt digne de protection, les personnes habilitées à invoquer l'une ou l'autre prétention prévues à l'article 30 al. 1 peuvent être **les proches de la personne** concernée ou encore **certaines associations** lorsqu'elles agissent pour défendre leurs intérêts propres ou celui de leurs membres (« recours égoïste » ; en allemand « egoistische Verbandsbeschwerde »). On retrouve la même solution en droit fédéral tant dans la loi actuelle (art. 25 al. 1) que dans le projet de révision (art. 37 al. 1)[11].

2. 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

[10] WALDMANN / OESCHGER, in Belser / Epiney / Waldmann (édit.), Datenschutzrecht – Grundlagen und öffentliches Recht, Berne 2011, § 13, n° 140 ss.
[11] A ce sujet, notamment : BANGERT Jan, in Maurer-Lambrou / Blechta (édit.), Basler Kommentar Datenschutzgesetz & Öffentllichkeitsgesetz, 3e éd., Bâle 2014, *ad* art. 25/25bis LPD, n° 29 ss.

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 peuvent par ailleurs être demandées. La nouveauté par rapport au droit actuel est l'introduction d'un nouveau droit à la **limitation du traitement**. Moins radicale que la rectification ou que la suppression des données, la limitation du traitement peut servir à limiter **temporairement** les effets d'une atteinte illicite en restreignant les possibilités de traiter certaines données, lorsque celles-ci ne peuvent pas être supprimées ou modifiées en raison d'un intérêt privé ou public prépondérant ou parce que le caractère illicite du traitement n'as pas encore pu être démontré. Concrètement, le responsable du traitement peut – respectivement doit – **continuer de conserver intactes** les données visées pendant toute la durée de la mesure, mais ne peut plus les traiter à d'autres fins jusqu'à ce que le motif ayant justifié la limitation du traitement ait pu être clarifié.

Art. 31, droit en cas de décision individuelle automatisée

1. Il existe plusieurs domaines dans lesquels des décisions peuvent aujourd'hui être rendues par un organe public sur la base d'un traitement automatisé de données **sans qu'un humain ne doive forcément intervenir**. On pense en particulier à l'émission d'une décision de taxation, à l'envoi d'une amende pour excès de vitesse, au versement de prestations d'assurance, à l'admission à un concours etc. Dans ces domaines, le recours aux outils technologiques permet **d'augmenter sensiblement** la capacité et le rythme de traitement des dossiers avec pour conséquence des économies significatives en terme de ressources. Toutefois, les algorithmes à la base de ces décisions ne sont **pas infaillibles** et peuvent se tromper. Il est donc important de compenser ce risque par des **garanties de procédure adaptées**.

2. Selon l'alinéa 1er de cette disposition, 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. L'alinéa 2 ajoute qu'à la demande de l'intéressé, 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**. L'alinéa 3 introduit la possibilité d'un réexamen extrajudiciaire **rapide et gratuit** des opérations de traitement liées à une décision automatisée, 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 qui l'a rendue. Sous l'angle procédural, la demande de réexamen suit les mêmes règles qu'en cas de **réclamation** au sens de l'article 103 CPJA. Les cas pour lesquels la loi prévoit déjà une procédure de réclamation sont réservés (par exemple : art. 174 ss LICD).

3. La nécessité d'introduire des garanties spécifiques relatives au prononcé de décisions individuelles automatisées découle des articles 11 Directive (UE) 2016/680 ; 22 Règlement (UE) 2016/679 et 9 § 1 let. c Convention STE 108+. En droit fédéral, de telles garanties sont

déjà prévues depuis plusieurs années à l'article 17a LPD et ont été réintroduites à l'article 19 p-LPD.

Art. 32, Réserve des codes de procédure

Les droits des personnes par rapport aux traitements de données personnelles qui sont effectués dans le cadre de procédures civiles, pénales et de juridiction administrative en cours obéissent au **droit de procédure applicable**. Le droit de procédure garantit la protection de la personnalité et des droits fondamentaux de toutes les personnes impliquées, offrant ainsi **une protection équivalente** à la législation sur la protection des données. En réglant le rapport entre la législation sur la protection des données et le droit de procédure, la règle évite le risque de conflits de normes et de contradictions, qui pourraient perturber le bon déroulement de la procédure. Elle correspond à la jurisprudence du Tribunal fédéral en la matière (cf. ATF 138 III 425, consid. 4.3).

Art. 33, Données de la personne décédée

Cette disposition introduit la possibilité pour toute personne de disposer du sort de ses données à caractère personnel **après sa mort**. Elle peut à cette fin charger un tiers de confiance ou s'adresser directement au responsable du traitement pour lui demander de procéder aux opérations de traitement qui devront être accomplies sur ses données le moment venu. Comme pour les autres droits en matière de protection des données, le droit de disposer de ses données après la mort n'est **pas absolu**. Il doit être pondéré avec les autres intérêts publics et privés entrant en ligne de compte. On retrouve une règle similaire notamment à l'article 16 p-LPD.

Art. 34, Procédure et voie de droit

Pas de commentaire.

Art. 35, Réparation du dommage et du tort moral

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

2.4 Chap. 4, Mise en œuvre de la protection des données

Art. 36 et 37, Responsabilités

1. L'article 36 ne subit **aucune modification** par rapport à la version actuelle de la loi. Comme c'est déjà le cas aujourd'hui, l'organe qui traite des données personnelles est responsable de leur protection et de leur sécurité. Cette responsabilité peut être partagée en interne, lorsqu'un même traitement implique la participation de plusieurs acteurs (cf. art. 4 let. g et 38 al. 1 let. h *in fine*). La question de la répartition des responsabilités en interne n'a cependant **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 d'un seul responsable de traitement.

2. L'article 37 règle les questions de responsabilité lorsqu'un organe public fait appel à la collaboration de personnes privées afin de traiter des données personnelles (**traitement sur mandat**). Les opérations de traitement qui sont confiées à une entreprise sous-traitante peuvent se dérouler soit directement dans le périmètre d'activité du responsable de traitement, ce qui suppose que l'entreprise sous-traitante utilise le matériel informatique de l'Etat, soit être entièrement externalisées sur les infrastructures et les systèmes informatiques de celle-ci, auquel cas on appliquera en sus l'article 13b sur **l'externalisation de données**.

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

Alinéa 2 – conformément à cette disposition, la transmission de données qui sont soumises à une obligation de confidentialité ne peuvent être confiées à un mandataire qu'à la condition que la confidentialité soit garantie non seulement à l'égard des tiers mais également à l'égard du mandataire lui-même. C'est le cas en particulier si les données transmises ont été cryptées et que le sous-traitant ne dispose pas de la clé de décryptage.

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

Art. 38 à 40, Registre des traitements et déclarations de traitements

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 de l'Etat, des communes et des Eglises reconnues.

2. 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. Chacune de ces dispositions sont largement similaires à ce que prévoit la LPrD actuellement.

3. Le registre des activités de traitement est **tenu par l'autorité cantonale de surveillance en matière de protection des données** (art. 40). Il est public et consultable gratuitement. Par rapport à la loi actuelle, l'avant-projet ajoute qu'il doit être disponible en ligne, ce qui

correspond déjà à ce qui se fait aujourd'hui[12]. Les communes qui le souhaitent peuvent tenir leur propre registre des activités de traitement ; elles sont cependant tenues de continuer d'annoncer leurs activités de traitement en sus à l'autorité cantonale de surveillance. Dans tous les cas, les communes doivent au minimum conserver chez elles une liste à jour de leurs activités de traitement qu'elles tiennent à la disposition du public (al. 2 et 3).

Art. 41, Mesures organisationnelles et techniques

1. Les responsables du traitement doivent prendre les mesures organisationnelles et techniques **appropriées** pour protéger les données personnelles qu'ils traitent contre les mauvaises manipulations, intentionnelles ou accidentelles, qui risquent d'en altérer la confidentialité, la disponibilité, l'authenticité ou l'intégrité.

2. 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 du règlement (UE) 2016/679 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 (al. 1) ;
b) être en mesure de **démontrer** aux autorités de surveillance et aux personnes concernées l'existence et la mise en œuvre de ces mesures au travers d'une documentation adaptée (al. 3).

3. Les mesures techniques et organisationnelles devant être mises en place concrètement par chaque responsable du traitement dépendent de **plusieurs critères** tels que le nombre et le type de données traitées, la fréquence et l'ampleur des traitements réalisés, les risques liés, mais aussi la taille de l'infrastructure, les ressources dont elle dispose et les technologies qu'elle utilise. 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 mobile.
L'ampleur du devoir de documenter dépend lui aussi des circonstances propres à chaque cas. Il peut prendre en particulier les formes suivantes : simple liste régulièrement actualisée des mesures techniques et organisationnelles mises en place, charte, politique, règlement d'utilisation *ad hoc* etc.

Art. 42, Protection des données dès la conception et par défaut

1. Les principes de la protection des données dès la conception et par défaut consacrent une approche qui prend en compte de **manière proactive la protection de** la vie privée tout au

[12] 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.

long du processus de traitement des données. Ils sont prévus dans la directive (UE) 2016/680 (art. 20 § 1), dans le règlement (UE) 2016/679 (art. 25) et dans la Convention STE 108+ (art. 10 § 2 et 3). Le Conseil fédéral les a aussi intégrés à l'article 6 du projet p-LPD.

2. Conformément au principe de la protection des données dès la conception (« ***privacy by design*** »), les responsables de traitement doivent intégrer des mesures de protection de la vie privée à **toutes les phases** du développement et de l'exploitation des systèmes et des applications traitant des données personnelles, incluant en particulier l'analyse, le design, la mise en œuvre, l'utilisation, le contrôle et la maintenance (al. 1). Les mesures à adopter dans ce domaine peuvent porter aussi bien sur des question d'ingénierie des systèmes que sur la mise en place de mesures techniques et organisationnelles (p. ex., le fait de définir à l'avance les données devant être collectées pour chaque type de traitement, le fait de fixer des échéances régulières pour effacer ou anonymiser des données personnelles ou encore le fait de mettre au point une procédure à suivre en cas de violation de la protection des données).

3. Selon le principe de la protection des données par défaut (« ***privacy by default*** »), les systèmes d'information et les applications traitant des données personnelles doivent être paramétrés, par défaut, de la manière **la plus favorable** à la protection de la vie privée (collecte limitée aux données strictement nécessaire à l'accomplissement de la tâche envisagée, communication ciblée de données plutôt qu'octroi d'un accès général à l'ensemble des données…).

Art. 43 et 44, 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 organismes : 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 règlement (UE) 2016/679), la Convention STE 108+ (art. 10 § 2) et le projet de révision de la LPD (art. 20), 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. 43 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 43 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 concret** pour les droits des personnes concernées nécessitant de prendre des mesures de protection particulières, le responsable du traitement doit consulter l'Autorité de la

transparence et de la protection des données avant d'être en droit de débuter le traitement (art. 44 al. 1). Cette dernière peut communiquer au responsable du traitement ses éventuelles objections et recommandations concernant le traitement envisagé (al. 2). Le responsable du traitement est **libre** de mettre en pratique ou non les recommandations de 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).

Art. 45 et 46, 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. 45 al. 1) ; *b)* consignation de la violation dans un document écrit (art. 45 al. 1 *in fine*) et *c)* annonce de la violation lorsque cela est nécessaire au ou à la préposée à la protection des données ou aux personnes concernées (art. 45 al. 2 et 3 et art. 46).

2. La loi n'exige pas que tout incident en matière de protection des données doive systématiquement être notifié au ou à la préposé-e à la protection des données. Seuls sont visés **les incidents entraînant un risque** pour les droits des personnes concernées. Il n'est toutefois pas nécessaire pour cela que le système d'information de l'organisme concerné ait fait l'objet d'une cyberattaque ; la simple perte d'une clé USB contenant des données personnelles sensibles peut, le cas échéant, déjà contraindre le responsable du traitement à faire une notification, si les personnes concernées peuvent être facilement identifiées. Même si la loi ne le dit pas expressément, le délai dans lequel doit intervenir la notification ne devrait en principe pas excéder 72 heures (comparaison : art. 30 § 1 Directive (UE) 2016/680 ; art. 33 § 1 Règlement (UE) 2016/670).

3. Lorsque la violation en cause est de nature à causer à une ou plusieurs personne(s) un préjudice, celle(s)-ci doivent en principe être **avertie(s) personnellement** (art. 46 al. 1). En cas d'inaction du responsable du traitement, l'annonce peut être ordonnée par le ou la préposé-e à la protection des données (al. 4). Pour les cas de violations qui touchent un grand nombre de personnes, il est possible de procéder au moyen d'une **annonce publique** que ce soit dans les journaux, à la télévision ou sur Internet (al. 3). Dans pareil cas, on veillera cependant à offrir aux personnes concernées la possibilité d'obtenir des informations plus précises et personnelles par la mise sur pied d'un point de contact. Exceptionnellement, le devoir d'annonce peut être différé, restreint ou supprimé dans certaines situations spécifiques (al. 2). Dans pareil cas, la notification au ou à la préposé-e reste néanmoins due, étant entendu que le secret de fonction ne peut pas lui être opposé (cf. art. 56 al. 3).

4. Conformément à l'article 45 al. 3, toute violation de la protection des données survenant chez un sous-traitant ou une sous-traitante, quelle que soit sa gravité, **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.

Art. 47, Correspondant et correspondante en matière de protection des données

1. L'avant-projet introduit l'obligation pour les organes publics qui traitent des données personnelles de désigner un correspondant ou une correspondante en matière de protection des données qui est chargé-e **de conseiller et d'accompagner** les responsables du traitement sous l'angle juridique dans le cadre de leurs activités. Une obligation similaire figure aux articles 32 ss de la Directive (UE) 2016/680 et aux articles 37 ss du Règlement (UE) 2016/679, qui exigent la désignation d'un « délégué à la protection des données ». En droit fédéral, le projet de révision de la LPD prévoit quant à lui à son article 9 al. 3 que les organes fédéraux devront nommer un « conseiller à la protection des données ».

2. Pour des raisons de proportionnalité et de pragmatisme, il n'est pas prévu d'étendre l'obligation de désigner un correspondant ou une correspondante en matière de protection des données à tout organe qui traite **ponctuellement** des données sur des personnes ; seuls sont visés les organes qui, dans le cadre de leurs activités ordinaires, traitent **régulièrement et systématiquement** des données à caractère personnel (al. 1). En outre, il n'est pas exigé que chaque unité administrative dispose de son propre correspondant ou de sa propre correspondante en matière de protection des données ; une seule et même personne peut accomplir cette fonction pour le compte de plusieurs unités administratives différentes au sein d'une même structure.

3. Le correspondant ou la correspondante en matière de protection des données assume avant toute chose un rôle de conseil ; il ou elle n'est **pas responsable** de la conformité des traitements (al. 3 *in fine*). Le correspondant ou la correspondante en matière de protection des données a cependant pour fonction de veiller à ce que les obligations qui se rapportent à la **mise en œuvre de la loi** soient correctement exécutées. C'est le cas en particulier du devoir d'annoncer les traitements au registre des activités de traitement (art. 38), du devoir de documenter les mesures techniques et organisationnelles mises en place (art. 41 al. 3), de l'obligation de réaliser une analyse d'impact avant de débuter certains types de traitement et de consulter, lorsque cela est nécessaire, l'autorité de surveillance (art. 43 et 44) et enfin du devoir de notifier les violations de la sécurité des données à l'autorité de surveillance, ainsi qu'aux personnes concernées (art. 45 et 46). Le correspondant ou la correspondante en matière de protection des données veille aussi à ce que les personnes qui exercent leurs droits en matière de protection des données obtiennent les réponses appropriées à leurs demandes de la part du responsable du traitement. Finalement, le correspondant ou la correspondante en matière de protection des données est **l'interlocuteur privilégié** de l'autorité de surveillance en matière de protection des données et fait ainsi la passerelle avec le responsable du traitement.

4. La disposition fixe **deux conditions** pour que le correspondant ou la correspondante en matière de protection des données puisse accomplir correctement ses fonctions :

a) d'une part, il faut qu'il ou elle soit en mesure de saisir les **principaux enjeux** relatifs à la protection des données et à sa mise en pratique (al. 3) ;
b) d'autre part, il est important qu'il ou elle soit **suffisamment associée** aux activités de traitement qui sont menées, les responsables du traitement devant lui communiquer d'office toutes les informations utiles à propos de leurs activités et répondre aux questions qui leurs sont adressées (al. 4).

2.5 Chap. 5, Surveillance

2.5.1 Section 5.1 : Autorités de surveillance en matière de protection des données

Art. 48, Autorité de surveillance

1. 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 conformément à l'alinéa 1er par l'Autorité cantonale de la transparence et de la protection des données (ci-après : l'Autorité cantonale).

2. Selon la loi actuelle, les **communes** ont la possibilité, pour autant qu'elles le souhaitent, de désigner leur propre autorité de surveillance en la matière. Cette possibilité a été reprise dans l'avant-projet (al. 2). Il est à relever cependant qu'à ce jour cette solution n'a été adoptée **par aucune commune**. Dans ces circonstances, on peut se poser la question si son maintien est justifié, ceci d'autant plus que les tâches à accomplir dans ce domaine deviennent de plus en plus complexes et nécessitent des ressources en conséquence. Si les retours de la consultation vont dans le sens d'une **suppression** de cette disposition, il conviendra en principe de supprimer également son pendant à l'art. 39 al. 4 LInf.

3. Par rapport à la situation actuelle, l'avant-projet prévoit que les **Eglises reconnues** qui ont adopté leurs propres règles en matière de protection des données sont tenues d'instituer également leur propre autorité de surveillance (al. 3). Ce changement va dans le sens d'une meilleure prise en considération de l'article 6 LEE, qui reconnaît **l'autonomie des Eglises** par rapport à l'Etat et aux communes. Il tient compte aussi des différences qu'il peut y avoir s'agissant du traitement des données personnelles à l'intérieur de l'Etat ou au sein d'une Eglise.

4. Les autorités de surveillances communales et ecclésiastiques doivent disposer de **compétences analogues** et présenter des **garanties similaires** à celles décrites dans la présente loi, notamment s'agissant de leur budget et de leur indépendance. En cas de manquement grave à ces exigences, l'Autorité cantonale peut se substituer à l'autorité de surveillance communale ou ecclésiastique. C'est dans cet optique également que, conformément à l'article 51 al. 1 let. f, l'Autorité cantonale continue **d'exercer la**

surveillance sur ces autorités-là à travers la Commission cantonale de la transparence et de la protection des données.

Art. 48 à 53, Organisation de l'Autorité cantonale de surveillance

1. L'avant-projet conserve la structure actuelle de l'Autorité cantonale de surveillance en matière de protection des données. Celle-ci se compose d'une part d'une **commission cantonale** et de l'autre d'un ou d'une **préposé-e à la protection des données** (cf. art. 29a al. 1 LPrD). Ce système a jusqu'ici permis de concilier efficacement l'indépendance vis-à-vis de l'administration et la légitimité tirées d'une commission élue par le Grand Conseil avec le professionnalisme d'une part, et la disponibilité quotidienne d'un ou une professionnel-le du droit de la protection des données, d'autre part. C'est pourquoi il est maintenu.

2. La composition et l'organisation de la Commission cantonale de la transparence et de la protection des données sont réglées à l'article 50. Celle-ci est un **organe pluridisciplinaire** réunissant plusieurs métiers et autant de compétences nécessaires à une compréhension la plus large possible des enjeux liés au domaine de la protection des données. Les membres de la commission **sont élus** par le Grand Conseil sur proposition du Conseil d'Etat. 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 (al. 2). Cet ajout correspond à la pratique actuelle: depuis son institution, la Commission de la transparence et de la protection des données a en effet toujours compté en son sein un ou une professionnel-le du droit.

3. Les attributions de la Commission sont énoncées à l'article 51. Il s'agit en particulier des fonctions de l'autorité de surveillance qui exigent une **légitimation accrue** : répondre aux consultations sur les projets d'acte législatif impliquant des traitements de données personnelles (let. d), prendre les décisions qui s'imposent à l'égard des responsables de traitement qui ne respectent pas les prescriptions légales applicables (let. e) ; haute surveillance sur les autres autorités du canton en matière de protection des données (let. f).

4. Le ou la préposé-e est un **spécialiste** du droit de la protection des données institué à l'article 52 de l'avant-projet. Il ou elle est nommé-e par le Conseil d'Etat sur préavis de la Commission. A nouveau, il s'agit d'un système qui permet de concilier dans toute la mesure du possible la légitimité, l'indépendance et le niveau de compétences requis. Par rapport aux autres employés de l'administration cantonale, le ou la préposé-e bénéficie d'un **statut spécial** qui déroge en partie aux règles ordinaires de la législation sur le personnel de l'Etat. A l'instar du Préposé fédéral à la protection des données (cf. art. 39 al. 5 du projet de révision de la LPD), il ou elle ne peut être évalué-e ni par l'Exécutif cantonal, ni par un autre organe de l'administration cantonale. Cette tâche a de ce fait été confiée à la Commission

qui dirige son activité (al. 2). De plus, les possibilités de résilier les rapports de fonction du ou de la préposé-e sont très restreintes (al. 3). Dans sa dernière recommandation suite à l'évaluation de 2018 de l'application par la Suisse de l'acquis de Schengen, le Conseil de l'Union européenne a demandé au canton de Lucerne de supprimer dans sa loi la possibilité de renvoyer le ou la préposé-e à la protection des données pour des « motifs justifiés » ne se limitant pas à la faute grave[13]. Ces spécificités sont nécessaires afin de **garantir l'indépendance** du ou de la préposée dans l'exercice de ses fonctions (cf. commentaire de l'art. 54).

5. Le ou la préposé-e à la protection des données assume l'essentiel de **l'activité courante** de surveillance et de conseil en matière de protection des données dans l'administration cantonale, auprès des communes et des particuliers. La liste de ses attributions figure à l'article 53 de l'avant-projet. Comme c'est déjà le cas actuellement, le ou la préposé-e est placé-e sous l'autorité de la Commission qui **dirige son activité** et qui peut à ce titre lui confier certains travaux spécifiques (art. 51 al. 1 let. a).

Art. 54, Indépendance et devoir de discrétion

1. La garantie d'indépendance de l'autorité de surveillance en matière de protection des données est une **exigence fondamentale** dans ce domaine 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 de la protection des données (cf. art. 42 de la Directive (UE) 2016/680 ; art. 52 du Règlement (UE) 216/679 ; art. 15 § 5 de la Convention STE 108 modernisée ; art. 26 al. 3 LPD et art. 39 al. 3 p-LPD). 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. Le critère de l'indépendance réunit **plusieurs éléments** qui ont été pris en compte soit de manière générale, soit de manière plus ciblée dans le cadre de la présente disposition :

a) *L'indépendance fonctionnelle* : l'autorité doit disposer des compétences nécessaires à l'accomplissement des tâches que la loi lui confie et ne doit pas être entravée dans l'exercice de ses fonctions ;

b) *L'indépendance institutionnelle* : l'autorité de surveillance ne doit pas recevoir de la part de l'Exécutif cantonal ou d'un autre organe de l'Etat d'instruction sur la manière d'exercer ses fonctions ;

c) *L'indépendance matérielle* : l'autorité de surveillance doit disposer des ressources humaines et matérielles nécessaires à l'accomplissement des tâches que la loi lui confie ;

[13] CONSEIL DE L'UNION EUROPÉENNE, *Décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2018 de l'application, par la Suisse, de l'acquis de Schengen dans le domaine de la protection des données*, 18 mars 2019, recommandation n° 2.

d) *indépendance personnelle* : les membres de l'autorité de surveillance ne doivent pas avoir des liens d'intérêts susceptibles d'influencer leur jugement par rapport aux tâches de protection des données qu'ils assument.

3. En outre, la disposition rappelle et précise que toute personne travaillant pour le compte de l'autorité de surveillance en matière de protection des données est soumise au secret de fonction et à l'obligation de discrétion (al. 4). Il s'ensuit que l'autorité **garantit l'anonymat** des demandes et des échanges qui lui sont adressés à moins que la personne concernée ne donne expressément son accord pour qu'ils soient divulgués, notamment auprès de l'organe qui serait suspecté d'une violation des prescriptions en matière de protection des données.

Art. 55, Autocontrôle de l'autorité de surveillance

Cette disposition oblige l'autorité de surveillance de 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, Moyens d'intervention

1. L'avant-projet prévoit de **renforcer les moyens d'intervention** de l'autorité de surveillance conformément aux nouveaux standards des lois de protection des données (cf. art. 47 § 2 de la Directive (UE) 2016/6890 et art. 58 § 2 du Règlement (UE) 2016/679 ; art. 15 § 2 let. a à d Convention STE 108+ et art. 44 et 45 p-LPD).

2. En plus des pouvoirs d'investigation et d'ester en justice ou de porter à la connaissance de l'autorité judiciaire les violations des dispositions de la protection des données, l'autorité de surveillance devra disposer à l'avenir de la compétence de **rendre des décisions contraignantes** pour les responsables du traitement. L'octroi d'une compétence décisionnelle à l'autorité de surveillance est un élément déterminant au sens de l'article 45 du Règlement (UE) 2016/679 pour décider du maintien de **la décision d'adéquation** de la Commission européenne en faveur de la Suisse. Elle fait partie **des recommandations** de cette même autorité suite à son évaluation, en 2018, de l'application par la Suisse de l'acquis de Schengen[14].

3. Les moyens d'intervention de l'autorité de surveillance ont été réparties en **deux catégories** : ceux qui reviennent directement au ou à la préposé-e à la protection des

[14] CONSEIL DE L'UNION EUROPÉENNE, *Décision d'exécution du Conseil arrêtant une recommandation pour remédier aux manquements constatés lors de l'évaluation de 2018 de l'application, par la Suisse, de l'acquis de Schengen dans le domaine de la protection des données*, 18 mars 2019, recommandation n° 3 et 4.

données et ceux qui sont du ressort de la Commission de la transparence et de la protection des données :

a) *Le ou la préposé- à la protection des données* 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 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 préposée 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 à une inspection sur place. Le secret de fonction ne peut pas lui être opposé (al. 3). S'il ou elle constate une violation des prescriptions de protection des données, le ou la préposé-e peut prononcer **une injonction** au responsable du traitement ou au sous-traitant afin qu'il mette son traitement en conformité avec les prescriptions légales (art. 57 al. 1). En cas de non-respect par le responsable du traitement d'une injonction du ou de la préposé-e, ce dernier ou cette dernière peut transmettre le cas à la Commission (al. 2).
b) En tant qu'organe collégial élu par le Grand Conseil, *la Commission de la transparence et de la protection des données* est l'organe compétent pour rendre **des décisions contraignantes** à l'égard des responsables du traitement (art. 58). Elle peut agit d'office ou peut être saisie par le ou la Préposé-e. La Commission peut ordonner différentes mesures allant de la suspension ou la modification du traitement jusqu'à 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**. A titre d'exemple, au lieu d'ordonner la cessation du traitement, la Commission peut ordonner sa modification et limiter la mesure à la partie du traitement qui pose problème. Si un responsable du traitement a omis de procéder à une analyse d'impact relative à la protection des données alors que les conditions d'une telle analyse sont réunies, la Commission peut ordonner la suspension du traitement jusqu'à ce que l'analyse d'impact ait été effectuée. Dans les cas **particulièrement graves** où les droits des personnes sont manifestement mis en danger par un traitement qui ne remplit de toute évidence pas les exigences légales, la Commission peut prononcer des **mesures provisionnelles** et ordonner la suspension du traitement jusqu'à droit connu sur le fond (al. 4).

4. Comme le prévoit l'article 59 al. 1 de l'avant-projet, tant le ou la préposé-e que la Commission de la transparence et de la protection des données respectent dans leurs interventions les règles du CPJA. En particulier, les mesures qui sont prononcées doivent l'être de manière **suffisamment précise** pour que le responsable du traitement soit en mesure de déterminer quels sont les traitements visés et les raisons qui ont motivé la mesure. La Commission de la transparence et de la protection des données ne siégeant pas de manière permanente et ne disposant pas de son propre personnel, il est prévu que le ou la préposé-e à la protection des données puisse **instruire** les affaires qui sont de la compétence la Commission. Celui-là ou celle-là agira dans ce cadre à la manière d'un greffier rapporteur ou d'une greffière rapporteuse avec voix consultative uniquement (art. 58 al. 5).

Art. 60 et 61, Coordination et coopération avec d'autres autorités

1. En plus des moyens d'actions directs dont dispose l'autorité de surveillance en matière de protection des données, l'avant-projet met également l'accent sur **la coordination et la coopération** avec les autres autorités cantonales de surveillance dans leur domaine de compétence respectif et les autres autorités de surveillance en matière de protection des données en Suisse et à l'étranger.

2. Lorsqu'une autorité administrative cantonale, quelle qu'elle soit, constate dans l'exercice de ses fonctions qu'un organe public extérieur à l'administration cantonale mais soumis à sa surveillance ne respecte pas les prescriptions de la loi sur la protection des données et que cette situation peut aboutir, le cas échéant, à une décision de sa part, elle est tenue d'inviter l'autorité de surveillance en matière de protection des données **à prendre position** (art. 60). Ce peut être le cas, par exemple, si l'autorité cantonale de la surveillance des notaires (la Commission du notariat) constate une carence en matière de protection des données auprès d'une personne soumise à sa surveillance. Si, après en avoir été informée, l'autorité de surveillance en matière de protection des données décide d'ouvrir une enquête, les deux autorités **doivent se coordonner entre elles**.

3. En vertu de l'article 61 de l'avant-projet, les autorités de surveillance en matière de protection des données en Suisse et aussi à l'étranger doivent **coopérer** dans la mesure nécessaire à l'accomplissement de leurs tâches, notamment en échangeant des informations relatives à des traitements effectués sur le territoire dont elles ont la charge. La coopération doit aussi porter sur la coordination de leurs investigations ou de leurs interventions, ainsi que sur la conduite d'actions conjointes. L'avant-projet prévoit que le type et l'étendue de la coopération doit faire l'objet d'une **convention écrite qui en détermine les contours**. A titre d'exemple de coopération, l'alinéa 3 prévoit expressément que l'autorité cantonale de surveillance peut intervenir auprès d'entreprises privées situées sur le territoire cantonal pour autant que le Préposé fédéral à la protection des données lui en ait confié le mandat.

Art. 62, Exception en faveur du pouvoir judiciaire

L'avant-projet supprimant l'exception selon laquelle la loi sur la protection des données ne s'applique pas de manière générale aux procédures juridictionnelles (cf. art. 2 al. 2 let. b de la loi actuelle), la présente disposition déclare que **l'autorité de surveillance en matière de protection des données n'est pas compétente** s'agissant des traitements effectués par les organes du pouvoir judiciaire dans l'exercice de leurs fonctions juridictionnelles. Cette dérogation, dont l'étendue est strictement limitée aux activités judiciaires proprement dites, a pour but de garantir la séparation des pouvoirs et l'indépendance de la justice. Elle est expressément prévue aux articles 45 § 2 Directive (UE) 2016/680 ; 55 § 3 règlement (UE) 2016/679 et 15 § 10 Convention STE 108+.

2.5.3 Section 5.3 : Autres tâches de l'autorité de surveillance

Art. 63, Registre des traitements

Conformément à cette disposition, la tenue correcte et à jour du registre des traitements mentionnés aux articles 38 à 40 de l'avant-projet est placée sous la responsabilité de l'Autorité cantonale de la transparence et de la protection des données. Les communes peuvent avoir leur propre registre. Mais dans ce cas, elles demeurent tenues de déclarer leurs traitements en plus à l'autorité cantonale de surveillance.

Art. 64, Rapport d'activité et information du public

1. L'obligation pour les autorités de surveillance en matière de protection des données d'établir un rapport d'activité est prévue aux articles 49 de la directive (UE) 2016/680 et 59 du Règlement (UE) 2016/679 ainsi qu'à l'article 15 § 7 Convention STE 108 modernisée. Elle existe déjà dans la loi actuelle à son article 30a al. 2. Au plan fédéral, l'obligation est mentionnée à l'article 30 al. 1 LPD et a été reprise à l'article 51 al. 1 p-LPD.

2. La faculté pour l'autorité de surveillance **d'informer le public** de ses constatations, lorsque l'intérêt général le justifie, est une conséquence de son **indépendance**. Selon un avis de droit de l'institut du fédéralisme portant précisément sur cette question dans le canton de Fribourg, l'autorité de surveillance peut délivrer des avis et rendre l'opinion publique attentive à des violations des principes de la protection des données, qui, de son point de vue, ont été commises par les autorités cantonales **sans devoir solliciter l'autorisation préalable** d'une autre autorité supérieure[15].

2.6 Chap. 6, Dispositions transitoires

Art. 65, Droit transitoire

1. Le passage au nouveau droit, notamment le renforcement des exigences en matière de sécurité à l'égard des responsables du traitement, ne peut à l'évidence pas se faire **sans un temps d'adaptation**. Il n'est pas non plus possible d'appliquer l'ensemble des nouvelles exigences à tous les traitements sans exception, alors qu'ils ont débuté à une époque où ce type d'exigence n'avait pas cours. C'est pourquoi l'avant-projet prévoit certaines dérogations et introduit des délais pour que les responsables du traitement se mettent en conformité avec le nouveau droit.

2. Tout d'abord, conformément à l'alinéa 3, les traitements ayant débuté sous l'ancien droit et qui sont terminés au moment de l'entrée en vigueur de la loi **continueront d'être soumis aux exigences de la LPrD de 1994**. En revanche, dans la mesure où cela est techniquement réalisable, les personnes concernées seront autorisées à invoquer l**es nouveaux droits**

[15] WALDMANN Bernhard / SPIELMANN Andre, L'indépendance de l'autorité cantonale de surveillance en matière de protection des données – Avis de droit réalisé sur mandat de la Direction de la Sécurité et de la Justice du canton de Fribourg, février 2010, n° 133.

prévus à la section 3 de la loi dès l'entrée en vigueur de la loi (droit d'accès élargi, droit d'opposition, droit de disposer de ses données après la mort). La même règle vaut pour les traitements de données en cours et futurs.

3. Selon l'alinéa 2, le principe de la protection des données dès la conception et les obligations relatives à la réalisation d'une analyse d'impact en matière de protection ne s'appliquent pas **aux traitements qui ont débuté sous l'ancien droit** et qui perdurent après l'entrée en vigueur du nouveau droit à condition que la finalité du traitement reste inchangée et qu'aucune nouvelle donnée n'est collectée. Cette règle se justifie dans la mesure où les devoirs des responsables du traitement prévus aux articles 42 à 44 s'appliquent surtout dans la phase préliminaire du traitement ; les responsables du traitement **ne doivent pas être obligés de les remplir rétroactivement**.

4. S'agissant des autres obligations, les responsables du traitement disposeront **d'un délai de deux ans** pour se mettre en conformité. Les annonces relatives à une violation de la protection 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).

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 de l'avant-projet (al. 4).

2.7 Adaptation de la législation spéciale

2.7.1 Adaptation de la LStat

Les modifications apportées aux articles 5 al. 1 et 16 al. 2 et 3 ont pour seul but de renvoyer à la nouvelle version de la loi sur la protection des données qui sera adoptée par le Grand Conseil.

2.7.2 Adaptation de la LJ

La modification de l'article 140 al. 1 let. c ne présente pas un lien direct avec la révision de la législation en matière de protection des données. Il s'agit d'une modification de cosmétique législative qui aurait en principe dû être introduite au moment de l'adoption de la LArch.

2.7.3 Adaptation de la LVid

La surveillance au moyen de caméras de vidéosurveillance de larges 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 43 et 44 de l'avant-projet (art. 4 al. 3).

2.7.4 Adaptation de la LGCyb

L'article 21 LGCyb concernant la tenue d'essai pilote est abrogé car la disposition a été insérée à l'article 21 de l'avant-projet de révision de la LPrD. Comme les deux dispositions ont un contenu similaire, les essais pilotes ayant été autorisés sous l'empire de l'article 21 LGCyb et qui se poursuivront, le cas échéant, au moment de l'entrée en vigueur de la présente disposition **ne sont pas impactés par ce changement**.

2.7.5 Adaptation de la LInf

En pratique, le ou la préposé-e à la protection des données et le ou la préposé-e à la transparence collaborent régulièrement lorsque se présente une demande d'accès à un document officiel qui contient également des données à caractère personnel. Le nouvel article 41 al. 2 let. c^{bis} vient codifier cette pratique au niveau de la loi.

2.7.6 Adaptation de la LS

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.

2.7.7 Adaptation de la LPol

1. Les modifications apportées dans la LPol servent pour l'essentiel à **mettre en conformité la législation fribourgeoise en matière de police** avec les exigences de la Directive (UE) 2016/680 qui est applicable en Suisse depuis le 25 août 2018.

2. L'article 38c al. 1 établit les conditions auxquelles il est possible de faire **du profilage** à des fins de prévention et de détection des infractions pénales. L'alinéa 2 est abrogé car les dispositions qu'il réserve entrent déjà dans le champ d'application de l'alinéa 1 let. a.

3. Les activités liées à la prévention, à la détection et à la poursuite d'infractions pénales impliquent nécessairement le traitement de données à caractère personnel concernant **différentes catégories** de personnes. L'article 38e al. 2 demande, dans la mesure du possible, **d'établir une distinction claire** entre les données à caractère personnel des différentes catégories de personnes concernées, telles que: les suspects, les personnes reconnues coupables d'une infraction pénale, les victimes et les autres parties, tels que les témoins et les personnes détenant des informations ou des contacts utiles. En outre, l'alinéa 3 réclame d'accorder une attention particulière au moment de rédiger les rapports de police afin de distinguer dans la mesure du possible **les données à caractère personnel qui sont fondées sur des faits de celles qui reposent sur des appréciations personnelles**. Ces deux obligations sont expressément prévues aux articles 6 et 7 de la Directive (UE) 2016/680.

4. A l'heure actuelle, il existe plusieurs bases données au niveau européen, suisse et intercantonal contenant des données nécessaires à l'accomplissement des tâches de police. L'article 38h fournit la base légale nécessaire pour que la police fribourgeoise puisse accéder à ces bases de données au moyen d'une **procédure d'appel**.

2.7.8 Adaptation de la LSan

Selon la modification apportée de 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 professionnel 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.

<u>Annexe</u> : ***Liste des principales abréviations***

Actes législatifs :

Ancienne 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).	2e modification de la LPD du 19 mars 2010	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).
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	LPDS	Loi sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal du 28 septembre 2018 (Loi sur la protection des données Schengen, LPDS ; RS 235.3)
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	p-LPD	Projet de loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois (FF 2017 6803)
Protocole additionnel à la Convention STE 108	Protocole additionnel à la Convention STE 108 du 8 novembre 2001 (RS 0.235.11).	LPrD	Loi cantonale fribourgeoise sur la protection des données du 25 novembre 1994 (RSF 17.1)
CPJA	Code de procédure et de juridiction administrative du canton de Fribourg du 23 mai 1991 (CPJA ; RSF 150.1).	Modification de la LPrD du 8 mai 2008	Loi modifiant la loi sur la protection des données (adaptation au droit international, en particulier aux accords Schengen/Dublin) (ROF 2008_053)

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).	LPol	Loi cantonale sur la police cantonale du 15 novembre 1990 (LPol ; RSF 551.1)
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.	LResp	Loi cantonale sur la responsabilité civile des collectivités publiques et de leurs agents (LResp ; RSF 16.1)
LArch	Loi cantonale sur l'archivage et les Archives de l'Etat du 10 septembre 2015 (LArch ; RSF 17.6).	LS	Loi cantonale sur la scolarité obligatoire du 9 septembre 2014 (LS ; RSF 411.0.1)
LCH	Loi cantonal fribourgeoise sur le contrôle des habitants du 23 mai 1986 (LCH ; RSF 114.21.1).	LSan	Loi cantonale sur la santé du 16 novembre 1999 (LSan ; RSF 821.0.1).
LEE	Loi fribourgeoise concernant les rapports entre les Eglises et l'Etat du 26 septembre 1990 (LEE ;RSF 190.1)	LSF	Loi fédérale sur la statistique fédérale du 9 octobre 1992 (LSF ; RS 431.01)
LGCyb	Loi cantonale fribourgeoise sur le guichet de cyberadministration de l'Etat du 2 novembre 2016 (LGCyb ; RSF 17.4)	LSR	Loi fédérale sur l'agrément et la surveillance des réviseurs du 16 décembre 2005 (LSR ; RS 221.302)
LICD	Loi sur les impôts cantonaux directs du 6 juin 2000 (LICD ; RSF 631.1)	LStat	Loi cantonale sur la statistique cantonale du 7 juillet 2006 (LStat ; RSF 110.1)
LInf	Loi sur l'information et l'accès aux documents du 9 septembre 2009 (RSF 17.5)	LTN	Loi fédérale concernant des mesures en matière de lutte contre le travail au noir (Loi sur le travail au noir, LTN ; RSF 822.41).
LJ	Loi cantonale sur la justice du 31 mai 2010 (LJ ; RSF 130.1)		
LOGA	Loi fédérale sur l'organisation du gouvernement et de l'administration du 21 mars 1997 (LOGA ; RS 172.010)	LTrans	Loi fédérale sur la transparence dans l'administration du 17 décembre 2004 (LTrans ; RS 152.3)

LPD	Loi fédérale sur la protection des données du 19 juin 1992 (LPD ; RS 235.1).	LVid	Loi cantonale sur la vidéosurveillance du 7 décembre 2010 (LVid ; RSF 17.3).
1ère modification de la LPD du 24 mars 2006	Modification du 24 mars 2006 de la loi fédérale sur la protection des données (RO 2007 4983)	RSD	Règlement sur la sécurité des données personnelles, du 29 juin 1999 (RSD ; RSF 17.15)

Autres abréviations :

ATF :	Arrêt du Tribunal fédéral
art. :	article
al. :	alinéa
cf. :	confer
Bako :	Basler Kommentar
BGC :	Bulletin officiel des séances du Grand Conseil
éd. :	édition
FF :	Feuille fédérale
RO :	Recueil officiel fédéral
ROF :	Recueil officiel fribourgeois
RSB :	Recueil systématique bernois
UE :	Union Européenne