Projet de loi modifiant la loi sur l'information du public, l'accès aux documents et la protection des données (LIPAD) A 2 08

Le GRAND CONSEIL de la République et canton de Genève
décrète ce qui suit :

Art. 1 **Modifications**

La loi sur l'information du public, l'accès aux documents et la protection des données, du 5 octobre 2001 (LIPAD – A 2 08), est modifiée comme suit :

Art. 3, al. 1, phrase introductive (nouvelle teneur), lettre c (nouvelle, la lettre c ancienne devenant la lettre d), lettre e (nouvelle teneur), lettre f (nouvelle), al. 2, phrase introductive (nouvelle teneur), al. 4 (nouvelle teneur)

[1] La présente loi s'applique aux institutions suivantes, sous réserve des alinéas 3 à 5 :

c) la Cour des comptes;
e) les groupements formés d'institutions visées aux lettres a, b et d ;
f) les personnes physiques ou morales et organismes chargés des tâches de droit public cantonal ou communal, dans les limites de l'accomplissement desdites tâches.

[2] Elle s'applique également, à l'exclusion du Titre III, aux personnes morales et autres organismes de droit privé sur lesquels une ou plusieurs des institutions visées à l'alinéa 1 exercent une maîtrise effective par le biais, alternativement :

[4] Le traitement de données personnelles effectué par la Banque Cantonale de Genève n'est pas soumis à la présente loi.

Art. 4, lettres b (nouvelle teneur), c (nouvelle teneur), d (nouvelle teneur), e (nouvelle teneur), f (nouvelle teneur), g (nouvelle teneur), h (nouvelle teneur), i (nouvelle, l'ancienne lettre i devenant la lettre n), j (nouvelle), k (nouvelle), l (nouvelle), m (nouvelle), o (nouvelle)

Dans la présente loi et ses règlements d'application, on entend par :

b) données personnelles sensibles, les données personnelles sur :
   1° les opinions ou activités religieuses, philosophiques, politiques ou syndicales,
   2° la santé, la sphère intime ou l'origine raciale ou ethnique,
   3° des mesures d'aide sociale,
   4° des poursuites ou sanctions pénales ou administratives;
   5° les données génétiques,
   6° les données biométriques identifiant une personne physique de façon unique,

c) profilage, toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects d'une personne, notamment pour analyser ou prédire des éléments concernant son rendement au travail, sa situation économique, sa santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses déplacements,

d) traitement, tout opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, l'enregistrement, la conservation, l'utilisation, l'extraction, la consultation, la modification, la communication, le rapprochement ou l'interconnexion, la limitation, l'effacement, la destruction ou l'archivage ;

e) communication, le fait de rendre accessibles des données personnelles ou un document, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant;

f) personne concernée, la personne physique ou morale au sujet de laquelle des données sont traitées;

g) responsable du traitement, institution au sens de l'article 3 qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles ;

h) sous-traitant, institution, organisme ou personne physique ou morale qui traite des données personnelles pour le compte du responsable du traitement ;

i) sécurité des données, ensemble des mesures organisationnelles et techniques permettant d'assurer la confidentialité, l'intégrité et la disponibilité des données ;
j) violation de la sécurité des données, toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données ;
k) anonymisation, traitement de données personnelles consistant à supprimer définitivement toutes les données identifiantes ou tout moyen de retrouver les données originales ;
l) pseudonymisation, traitement de données personnelles consistant à remplacer l'ensemble des données identifiantes par un identifiant neutre (pseudonyme), de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires ;
m) caviardage, traitement de données personnelles consistant à masquer des passages ou des données d'un document en vue de sa communication ou de sa publication ;
n) numéro d'identification personnel commun, le numéro commun à deux ou plusieurs institutions constitué d'une suite de chiffres, comprenant cas échéant des lettres et signes, qui est destiné à identifier des personnes physiques ou morales recensées auprès de ces institutions ;
o) décision individuelle automatisée, toute décision prise exclusivement sur la base d'un traitement de données automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

Section 4A Cour des comptes (nouvelle)

Art. 13A Huis clos (nouveau)

Les délibérations et autres séances de la Cour des comptes se tiennent à huis clos.

Art. 20A Cour des comptes (nouveau)

[1] La Cour des comptes informe par le biais de la publication de ses rapports et d'autres documents qu'elle considère d'intérêt public. Elle veille à la protection du secret professionnel, de fonction, fiscal, ou d'affaires des personnes entendues et de tout autre secret prévu par la loi.

[2] Sans préjudice de l'application des lois régissant ses activités, la Cour des comptes ne peut donner d'informations susceptibles de permettre

l'identification de l'auteur d'une communication ou d'une personne qu'elle a entendue.

[3] Elle veille au respect des règles professionnelles prohibant la transmission d'informations ou la transmission de documents en matière d'audit, d'évaluation ou de révision.

Art. 26, al. 2 let. d (nouvelle teneur)

[2] Tel est le cas, notamment, lorsque l'accès aux documents est propre à :

d) compromettre l'ouverture, le déroulement ou l'aboutissement d'enquêtes ou d'investigations prévues par la loi ;

Art. 28, al. 3 (nouveau, les alinéas 3 à 7 anciens devenant les alinéas 4 à 8) (nouvelle teneur), al. 4 (nouvelle teneur), al. 6 (nouvelle teneur), al. 7 (nouvelle teneur)

[3] Lorsque plusieurs demandes d'accès portent sur un même document détenu par plusieurs institutions, ces dernières déterminent laquelle traite la demande, et en informent la requérante ou le requérant. Les autres demandes deviennent sans objet.

[4] En cas de doute sur la réalisation d'une des exceptions prévues à l'article 26, la personne qui est saisie de la demande d'accès doit en référer à la conseillère ou au conseiller à la protection des données et à la transparence désigné conformément aux mesures d'organisation et de procédure prévues à l'article 50.

[6] Lorsqu'une institution entend donner accès à un document nonobstant l'opposition d'une autre institution ou d'un tiers, elle leur indique qu'ils peuvent saisir la préposée cantonale ou le préposé cantonal préalablement à toute communication. Elle confirme son intention par écrit en indiquant le délai figurant à l'article 30, alinéa 2, et en informe la préposée cantonale ou le préposé cantonal.

[7] Lorsqu'une institution entend rejeter une demande d'accès, elle en informe la requérante ou le requérant en lui indiquant qu'elle ou il peut saisir la préposée cantonale ou le préposé cantonal. Elle lui confirme son intention par écrit en indiquant le délai figurant à l'article 30, alinéa 2.

Art. 30, al. 1, phrase introductive et let. a (nouvelle teneur), al. 2 (nouvelle teneur), al. 3 (nouvelle teneur), al. 5 (nouvelle teneur)

[1] La préposée cantonale ou le préposé cantonal est saisi par une requête écrite de médiation sommairement motivée, à l'initiative :

a) d'une requérante ou d'un requérant dont la demande d'accès à un document n'est pas satisfaite;

[2] Le délai pour saisir la préposée cantonale ou le préposé cantonal est de 10 jours à compter de la confirmation écrite de l'intention de l'institution prévue à l'article 28, alinéas 5 et 6. Si une institution tarde à se déterminer sur une demande d'accès à un document, la requérante ou le requérant ou l'opposante ou l'opposant à la demande d'accès peuvent saisir la préposée cantonale ou le préposé cantonal.

[3] La préposée cantonale ou le préposé cantonal recueille de manière informelle l'avis des institutions et personnes concernées. La consultation sur place des documents faisant l'objet d'une requête de médiation ne peut lui être refusée, à charge pour lui de veiller à leur absolue confidentialité et de prendre, à l'égard tant des parties à la procédure de médiation que des tiers et du public, toutes mesures nécessaires au maintien de cette confidentialité aussi longtemps que l'accès à ces documents n'a pas été accordé par une décision ou un jugement définitifs et exécutoires.

[5] A défaut, la préposée cantonale ou le préposé cantonal formule, à l'adresse de la requérante ou du requérant ainsi que de l'institution ou des institutions concernées, une recommandation écrite sur la communication du document considéré. L'institution concernée rend alors dans les 10 jours une décision sur la communication du document considéré. Elle notifie aussi sa décision à la préposée cantonale ou au préposé cantonal.

Art. 33, al. 3 (nouvelle teneur)

[3] La rectification consiste dans la publication gratuite dans le média considéré, à bref délai et sans modification, d'un texte rectificatif factuel, véridique, concis et clair soumis par l'institution compétente, dans des conditions d'insertion et de présentation comparables à celles ayant entouré la présentation des faits en question. La publication comporte la précision que le texte rectificatif émane de l'institution requérante, et elle peut être accompagnée, de la part de l'éditeur, d'une déclaration quant au maintien ou non de sa présentation des faits et de l'indication de ses sources.

Art. 35 Principes (nouvelle teneur avec modification de la note)

[1] Tout traitement de données personnelles doit être licite.

[2] Il doit être conforme aux principes de la bonne foi et de la proportionnalité.

[3] Les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités ; sont

réservés les cas dans lesquels la personne concernée a consenti à un changement de finalité.

[4] Elles sont détruites, effacées ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi. Sur décision de l'institution concernée, la destruction de données personnelles peut être différée durant deux ans au maximum à des fins d'évaluation de politiques publiques.

[5] Quiconque traite des données personnelles doit s'assurer qu'elles sont exactes. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées.

[6] Lorsqu'une institution constate que des données personnelles qu'une autre institution lui a communiquées en vertu de l'article 39, alinéa 1 ou d'une autre base légale, sont inexactes, incomplètes ou obsolètes, elle en informe cette dernière, à moins que cette information ne soit contraire à une loi ou un règlement.

Art. 36 Base légale (nouvelle teneur avec modification de la note)

[1] Les institutions ne peuvent traiter des données personnelles que si une base légale le prévoit ou si l'accomplissement de leurs tâches légales le rend nécessaire.

[2] Les traitements de données personnelles sensibles, les activités de profilage et les traitements de données personnelles dont les finalités ou les modalités de traitement sont susceptibles de porter gravement atteinte aux droits fondamentaux de la personne concernée ne peuvent avoir lieu que si :

a) une loi au sens formel le prévoit expressément, ou
b) le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel.

[3] L'article 36A est réservé.

[4] Un numéro d'identification personnel commun ne peut être utilisé que s'il est institué par une loi cantonale. L'usage et la communication du numéro AVS sont régis par la loi fédérale sur l'assurance-vieillesse et survivants, du 20 décembre 1946.

Art. 36A Consentement (nouveau)

[1] En dérogation à l'article 36, les institutions peuvent traiter des données personnelles, y compris sensibles, nécessaires à l'accomplissement de leurs tâches légales, si la personne concernée a consenti au traitement en l'espèce.

Le responsable du traitement doit être en mesure de démontrer l'existence d'un tel consentement.

[2] La personne concernée ne consent valablement que si elle exprime librement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée. Le consentement doit être exprès en cas de traitement de données personnelles sensibles ou de profilage.

[3] Le consentement peut être révoqué en tout temps et sans motifs. La mise en œuvre effective du retrait du consentement peut toutefois requérir un délai raisonnable pour des raisons techniques.

[4] Dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement, les institutions peuvent traiter des données personnelles si le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

[5] Les institutions peuvent également traiter des données personnelles, y compris sensibles, en dérogation à l'article 36, si la personne concernée a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement.

Art. 36B Traitement conjoint (nouveau)

Lorsque deux institutions ou plus déterminent conjointement les finalités et les moyens du traitement, elles sont responsables conjointes du traitement et doivent définir de manière transparente leurs obligations respectives dans la déclaration au sens de l'article 43.

Art. 36C Sous-traitant (nouveau)

[1] Le traitement de données personnelles peut être confié à un sous-traitant pour autant qu'un contrat ou la loi le prévoie et que les conditions suivantes soient réunies :

a. seuls sont effectués les traitements que le responsable du traitement est en droit de réaliser ;
b. aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

[2] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou public en la forme écrite, prévoyant pour chaque étape du traitement le respect des prescriptions de la présente loi et du règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant. Les cas où la loi prévoit en détail les modalités de la sous-traitance sont réservés.

[3] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit du responsable du

traitement et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.
[4] Le responsable du traitement demeure responsable des données personnelles qu'il fait traiter au même titre que s'il les traitait lui-même.
[5] S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si l'Etat concerné dispose d'une législation assurant un niveau de protection adéquat conformément à la liste établie par le Conseil fédéral.

Art. 37 Protection des données dès la conception et par défaut (nouveau, l'art. 37 ancien devenant l'art. 37A)

[1] Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes fixés à l'article 35. Il le fait dès la conception du traitement.
[2] Les mesures organisationnelles et techniques doivent être appropriées au regard notamment de l'état de la technique, du type de traitement et de son étendue, ainsi que du risque que le traitement des données présente pour la personnalité ou les droits fondamentaux des personnes concernées.
[3] Le responsable du traitement est tenu de garantir, par le biais de préréglages appropriés, que le traitement soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

Art. 37A Sécurité des données personnelles (nouvelle teneur)

[1] Les institutions doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru.
[2] Les mesures doivent permettre d'éviter toute violation de la sécurité des données personnelles.
[3] Le Conseil d'Etat détermine, par voie règlementaire, les exigences minimales en matière de sécurité des données.
[4] Les institutions sont tenues de contrôler périodiquement le respect des mesures de sécurité mises en place au sens du présent article.

Art. 37B Analyse d'impact (nouveau)

[1] Lorsqu'un traitement de données est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer

plusieurs opérations de traitement semblables, il peut établir une analyse d'impact commune.

[2] L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants :

a. traitements de données sensibles à grande échelle ;
b. profilage;
c. surveillance systématique de grandes parties du domaine public.

[3] L'analyse d'impact contient notamment :

a. une description du traitement envisagé ;
b. une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée ; ainsi que
c. les mesures prévues pour protéger la personnalité et les droits fondamentaux de la personne concernée.

[4] Lorsque l'analyse d'impact est requise selon l'alinéa 1, elle est jointe au projet d'acte législatif pour avis de la préposée cantonale ou du préposé cantonal au sens de l'article 56, alinéa 3, lettre e de la loi.

Art. 37C Violation de la sécurité des données (nouveau)

[1] Lorsqu'il constate une violation de la sécurité des données, le responsable du traitement prend immédiatement les mesures appropriées afin de mettre fin à la violation et d'en minimiser les effets, et en informe immédiatement sa conseillère ou son conseiller à la protection des données et à la transparence au sens de l'article 50.

[2] Il consigne dans un document interne la nature de la violation, le type de données concernées et les catégories de personnes touchées, les conséquences probables pour ces dernières et les mesures prises pour y remédier.

[3] Le responsable du traitement annonce dans les meilleurs délais à la préposée cantonale ou au préposé cantonal, par l'intermédiaire de sa conseillère ou de son conseiller à la protection des données et à la transparence, les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

[4] Le responsable du traitement informe la personne concernée lorsque cela est nécessaire à sa protection ou lorsque la préposée cantonale ou le préposé cantonal l'exige.

[5] Il peut restreindre l'information de la personne concernée, la différer ou y renoncer, dans les cas suivants :

a. les intérêts prépondérants d'un tiers l'exigent ;

b. un intérêt public prépondérant l'exige, en particulier la sécurité intérieure ou l'ordre public ;
c. un devoir légal de garder un secret spécial l'interdit ;
d. la communication des informations est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative ;
e. l'information est impossible à fournir ou exige des efforts disproportionnés ;
f. l'information de la personne concernée peut être garantie de manière équivalente par une communication publique.

Art. 38 Devoir d'informer lors de la collecte de données personnelles (nouvelle teneur avec modification de la note)

[1] Le responsable du traitement informe la personne concernée de manière adéquate de la collecte de données personnelles la concernant, que celle-ci soit effectuée auprès d'elle ou non.

[2] L'information doit porter au moins sur les éléments suivants :
a. le responsable du traitement ;
b. la finalité du traitement ;
c. le cas échéant, les destinataires ou les catégories de destinataires auxquelles des données personnelles sont transmises ;
d. les catégories de données traitées.

[3] Lorsque des données personnelles sont communiquées à l'étranger, le responsable du traitement communique également à la personne concernée le nom de la corporation ou de l'établissement de droit public auquel elles sont communiquées et, le cas échéant, l'application d'une des exceptions prévues à l'article 39, alinéa 7.

[4] Si les données personnelles ne sont pas collectées auprès de la personne concernée, le responsable du traitement lui communique les informations mentionnées aux alinéas 2 à 3 dans les meilleurs délais, mais au plus tard lors de leur première utilisation.

Art. 38A Exceptions au devoir d'informer lors de la collecte de données personnelles (nouveau)

[1] Le responsable du traitement est délié du devoir d'information au sens de l'article 38 si l'une des conditions suivantes est remplie :
a. la personne concernée dispose déjà des informations au sens de l'article 38 ;
b. le traitement des données personnelles est prévu par la loi;
c. l'information n'est pas possible ou exige un effort disproportionné.

[2] Le responsable du traitement peut restreindre ou différer la communication des informations, ou y renoncer, si un intérêt public ou privé prépondérant le justifie, en particulier dans les cas prévus à l'article 46 de la présente loi.

Art. 38B Droits de la personne concernée en cas de décision individuelle automatisée (nouveau)

[1] Le responsable du traitement informe la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative.

[2] A la demande de la personne faisant l'objet d'une décision individuelle automatisée, le responsable du traitement lui communique la logique et les critères à la base de celle-ci. Cette demande ne suspend pas le délai visé à l'alinéa 3.

[3] Toute personne faisant l'objet d'une décision individuelle automatisée peut former une réclamation, dans les 30 jours à compter de sa notification, auprès de son auteur.

[4] La décision sur réclamation ne peut pas être rendue de manière automatisée.

[5] Les dispositions de la législation spéciale qui prévoient déjà une procédure de réclamation sont réservées.

Art. 39, al. 1, phrase introductive (nouvelle teneur), al. 2 (nouvelle teneur), al. 3 (nouvelle teneur), al. 5 (nouvelle teneur), al. 7, let. b (nouvelle teneur), al. 8 (nouvelle teneur), al. 9, let. b (nouvelle teneur), al. 10 (nouvelle teneur), al. 11 (nouvelle teneur)

A une autre institution soumise à la loi

[1] Sans préjudice, le cas échéant, de son devoir de renseigner les instances hiérarchiques supérieures dont elle dépend, une institution ne peut communiquer des données personnelles en son sein ou à une autre institution que si, cumulativement :

[2] L'institution requise est tenue de s'assurer du respect des conditions posées à l'alinéa 1 et, une fois la communication effectuée, d'en informer sa conseillère ou son conseiller à la protection des données, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement.

[5] L'institution requise est tenue de s'assurer du respect des conditions posées à l'alinéa 4 et, avant de procéder à la communication requise, d'en informer sa conseillère ou son conseiller à la protection des données et à la

transparence, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement. S'il y a lieu, il assortit la communication de charges et conditions.

[7] En l'absence du niveau de protection des données requis par l'alinéa précédent, la communication n'est possible que si elle n'est pas contraire à une loi ou un règlement et si, alternativement :

b) elle est dictée par un intérêt public important manifestement prépondérant reconnu par l'institution requise et que l'entité requérante fournit des garanties fiables suffisantes quant au respect des droits fondamentaux de la personne concernée;

[8] L'institution requise est tenue de consulter la préposée cantonale ou le préposé cantonal avant toute communication. S'il y a lieu, elle assortit la communication de charges ou conditions.

[9] La communication de données personnelles à une tierce personne de droit privé n'est possible, alternativement, que si :

b) un intérêt privé digne de protection de la requérante ou du requérant le justifie sans qu'un intérêt prépondérant des personnes concernées ne s'y oppose.

[10] Dans les cas visés à l'alinéa 9, lettre b, l'institution requise est tenue de consulter les personnes concernées avant toute communication, à moins que cela n'implique un travail disproportionné. A défaut d'avoir pu recueillir cette détermination, ou en cas d'opposition d'une personne consultée, l'institution requise sollicite le préavis de la préposée cantonale ou du préposé cantonal. La communication peut être assortie de charges et conditions, notamment pour garantir un niveau de protection adéquat des données.

[11] Outre aux parties, l'institution requise communique sa décision aux personnes consultées ainsi qu'à la préposée cantonale ou au préposé cantonal.

Art. 41 Traitement à des fins générales ne se rapportant pas à des personnes (nouvelle teneur avec modification de la note)

[1] Les institutions soumises à la présente loi sont en droit de traiter des données personnelles à des fins générales de statistique, de recherche scientifique, de planification ou d'évaluation de politiques publiques, indépendamment des buts pour lesquels elles ont été collectées, si les conditions suivantes sont réunies:

a) les données sont rendues anonymes dès que la finalité du traitement le permet;

b) l'institution ne communique les données sensibles à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées;
c) le destinataire ne communique les données à des tiers qu'avec le consentement de l'institution qui les lui a transmises;
d) les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier les personnes concernées .

[2] Les articles 35, alinéa 3, 36, alinéa 2 et 39 ne sont pas applicables.

Art. 43 Registre des activités de traitement (nouvelle teneur avec modification de la note)

[1] La préposée cantonale ou le préposé cantonal dresse et tient à jour un registre public des activités de traitement des institutions. Il le rend facilement accessible.

[2] Les institutions déclarent leurs activités de traitement à la préposée cantonale ou au préposé cantonal, en fournissant au moins les indications suivantes :

a. la ou le responsable du traitement ;
b. la dénomination, la base légale et la finalité du traitement ;
c. une description des catégories des personnes concernées et des catégories des données personnelles traitées ;
d. les catégories des destinataires ;
e. le cas échéant, l'identité et les coordonnées des autres responsables du traitement ;
f. le cas échéant, l'identité et les coordonnées des sous-traitants.

[3] Les institutions fournissent également les indications suivantes à la préposée cantonale ou au préposé cantonal, sur requête de ces derniers :

a. dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation ;
b. dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l'article 37A ;
c. en cas de communication de données personnelles à l'étranger, le nom de l'Etat ou de l'organisme international destinataire et, le cas échéant, l'application d'une des exceptions prévues à l'article 39, alinéa 7 .

[4] Le Conseil d'Etat peut prévoir des exceptions à l'obligation de déclarer pour certaines catégories de traitement à des fins administratives internes qui ne présentent manifestement pas de risques pour les droits des personnes concernées.

Art. 44 Principes (nouvelle teneur)

[1] Toute personne physique ou morale de droit privé peut demander par écrit au responsable du traitement si des données la concernant sont traitées.

[2] La personne reçoit les informations nécessaires à la mise en œuvre de ses droits en matière de protection des données personnelles. A sa demande, elle reçoit notamment les informations suivantes :

a. les coordonnées du responsable du traitement ;
b. les données personnelles traitées ;
c. la finalité du traitement ;
d. la durée de conservation des données personnelles, ou, si cela n'est pas possible, les critères pour fixer cette dernière ;
e. les informations disponibles sur l'origine des données personnelles, dans la mesure où ces données n'ont pas été collectées auprès de la personne concernée ;
f. le cas échéant, les destinataires ou les catégories de destinataires auxquels des données sont communiquées, ainsi que l'application d'une des exceptions prévues à l'article 39, alinéa 7.

[3] L'institution publique qui fait traiter des données par un sous-traitant demeure tenue de communiquer les données et de fournir les informations demandées.

[4] Nul ne peut renoncer par avance à son droit d'accès.

Art. 45 Modalités (nouvelle teneur)

[1] La personne qui fait valoir son droit d'accès doit justifier de son identité.

[2] Les renseignements sont, en règle générale, fournis par écrit sur un support physique ou électronique. En accord avec le responsable du traitement, la personne concernée peut également consulter ses données sur place.

[3] Le responsable du traitement fournit gratuitement les renseignements demandés. Le Conseil d'Etat peut prévoir des exceptions, notamment si la communication de l'information implique un travail disproportionné.

[4] A moins que des circonstances exceptionnelles le justifient, les renseignements sont fournis dans un délai de 30 jours.

Art. 47, al. 1, phrase introductive (nouvelle teneur), al. 2 (nouvelle teneur)

[1] Toute personne physique ou morale de droit privé peut, à propos des données la concernant, exiger des institutions qu'elles :

[2] Sauf disposition légale contraire, elle est en particulier en droit d'obtenir des institutions, à propos des données la concernant, qu'elles :

a) effacent ou détruisent celles qui ne sont pas nécessaires ;

b) rectifient, complètent ou mettent à jour celles qui sont respectivement inexactes, incomplètes ou dépassées;
c) fassent figurer, en regard de celles dont ni l'exactitude ni l'inexactitude ne peuvent être prouvées, une mention appropriée, à transmettre également lors de leur communication éventuelle;
d) s'abstiennent de communiquer celles qui ne répondent pas aux exigences de qualité visées à l'article 35 ;
e) publient leur décision prise suite à sa requête ou la communiquent aux institutions ou tiers ayant reçu de leur part des données ne répondant pas aux exigences de qualité visées à l'article 35;

Art. 49, al. 1 (nouvelle teneur), al. 3, 4, et 5 (abrogés), al. 6 (nouvelle teneur)

[1] Toute requête fondée sur les articles 44, 47 ou 48 doit être adressée par écrit au responsable du traitement dont relève le traitement considéré.

[6] L'institution concernée statue par voie de décision dans les 30 jours sur les prétentions de la requérante ou du requérant. Elle notifie aussi sa décision à la préposée cantonale ou au préposé cantonal.

Art. 50 Conseillères et conseillers à la protection des données et à la transparence et procédures (modification de la note), al. 1 (nouvelle teneur), al. 2, let. e (nouvelle teneur, les alinéas e à i anciens devenant les alinéas f à j), al. 3 (nouvelle teneur), al. 5 (nouvelle teneur)

[1] Des conseillères et conseillers à la protection des données et à la transparence (ci-après : conseillères et conseillers LIPAD) ayant une formation appropriée et les compétences utiles sont désignés et des procédures sont mises en place au sein des institutions, pour y garantir une correcte application de la présente loi.

[2] Les mesures d'organisation générales et les procédures visées à l'alinéa 1 sont adoptées, après consultation de la préposée cantonale ou du préposé cantonal, par les instances suivantes :
e) la Cour des comptes pour elle-même;

[3] Sur préavis de la préposée cantonale ou du préposé cantonal, le Conseil d'Etat prescrit par substitution les mesures d'organisation générales et les procédures nécessaires à une correcte application du titre III de la présente loi, si une instance visée à l'alinéa 3, lettres f à j, n'en adopte pas en temps utile après avoir été mise en demeure de le faire.

[5] La liste des conseillères et conseillers LIPAD désignés en application du présent article est publique.

Art. 51, al. 1 (nouveau, l'al. 1 ancien devenant l'al. 5), al. 2 (nouveau, l'al. 2 ancien devant l'al. 4), al. 3 (nouvelle teneur), al. 4 (nouvelle teneur)

[1] Les conseillères et conseillers LIPAD sont les interlocuteurs des personnes concernées et de la préposée cantonale ou du préposé cantonal pour tout ce qui a trait au traitement des données personnelles et à la transparence de l'institution qui les a désignés.

[2] Ils ont une fonction de conseil et de soutien et sont associés de manière appropriée aux activités de traitement accomplies au sein de l'institution.

[3] Ils accomplissent en particulier les tâches suivantes :

a) donner aux membres de l'institution les instructions utiles sur le traitement des données personnelles nécessaires à l'accomplissement de leurs tâches légales ou des demandes d'accès aux documents ;
b) concourir à l'établissement de l'analyse d'impact relative à la protection des données ;
c) communiquer à la préposée cantonale ou au préposé cantonal la liste des activités de traitement de l'institution au sens de l'article 43 de la présente loi, ainsi que ses mises à jour régulières ;
d) annoncer à la préposée cantonale ou au préposé cantonal les violations de la sécurité des données qui leur ont été communiquées par le responsable du traitement.

[4] Les conseillères et conseillers LIPAD détiennent, à l'égard des membres de l'institution à laquelle ils appartiennent, la compétence :

a) d'exiger d'eux tous renseignements utiles sur le traitement des données personnelles ou celui des demandes d'accès aux documents régies par la présente loi, qu'ils effectuent ou sont appelés à effectuer ;
b) de prendre par voie d'évocation les décisions d'application de la présente loi entrant ordinairement dans leur sphère de compétence.

[5] Les membres des institutions informent leur conseillère ou conseiller LIPAD, notamment :

a) de tout nouveau traitement de données;
b) de toute requête de communication et de toute intention de destruction de données personnelles, à moins que ces opérations ne soient prévues explicitement par une loi, un règlement ou une décision du Conseil d'Etat;
c) de toute information ou consultation qu'ils adressent directement à la préposée cantonale ou au préposé cantonal.

Art. 52, al. 1 (nouvelle teneur), al. 2 et 3 (nouveaux)

[1] Afin de garantir une application coordonnée des principes applicables en matière d'information relative aux activités des institutions et de ceux régissant la protection des données personnelles, il est institué la fonction de préposée cantonale ou de préposé cantonal à la protection des données et à la transparence.

[2] La préposée cantonale ou le préposé cantonal se concerte avec l'archiviste d'Etat lorsque l'application de la présente loi implique celle de la loi sur les archives publiques, du 1er décembre 2000.

[3] Il entretient des contacts réguliers avec la commission consultative.

Art. 55A Autocontrôle (nouveau)

La préposée cantonale ou le préposé cantonal s'assure, par des mesures de contrôle appropriées portant notamment sur la sécurité des données personnelles, du respect et de la bonne application des dispositions de la présente loi en son sein.

Art. 56 Compétences de la préposée cantonale ou du préposé cantonal en matière d'information du public et d'accès aux documents (nouvelle teneur avec modification de la note)

[1] La préposée cantonale ou le préposé cantonal surveille l'application de la présente loi en matière d'information du public et d'accès aux documents.

[2] Elle ou il est chargé, en application du titre II de la présente loi :

a) de traiter les requêtes de médiation relatives à l'accès aux documents;
b) d'informer d'office ou sur demande sur les modalités d'accès aux documents;
c) de centraliser les normes et directives que les institutions édictent pour assurer l'application de l'article 50;
d) de collecter les données utiles pour évaluer l'effectivité et l'efficacité de la mise en œuvre de la présente loi;
e) d'exprimer son avis sur les projets d'actes législatifs ayant un impact en matière de transparence.

Art. 56A Compétences de la préposée cantonale ou du préposé cantonal en matière de protection des données personnelles (nouveau)

[1] La préposée cantonale ou le préposé cantonal surveille l'application de la présente loi en matière de protection des données personnelles, notamment en procédant à des contrôles auprès des institutions.

[2] Elle ou il a la charge, en vertu du titre III de la présente loi :

a) d'émettre les préavis requis en vertu de la présente loi;

b) de collecter et centraliser les avis et informations que les institutions, ou leurs conseillères et conseillers LIPAD, doivent lui fournir, et, s'il y a lieu, de prendre position dans l'exercice de ses compétences;
c) de conseiller les instances compétentes des institutions sur les mesures d'organisation et les procédures à prescrire en leur sein;
d) d'assister les conseillères et conseillers LIPAD dans l'accomplissement de leurs tâches;
e) d'exprimer son avis sur les projets d'actes législatifs ayant un impact en matière de protection des données personnelles;
f) de dresser, mettre à jour et rendre accessible au public le catalogue des traitements des institutions;
g) de dresser, mettre à jour et rendre accessible au public la liste des conseillères et conseillers LIPAD désignés au sein des institutions;
h) de renseigner d'office ou sur demande les personnes concernées sur leurs droits;
i) d'exercer le droit de recours prévu à l'article 62, ainsi que dans les autres cas prévus dans la loi.

Art. 56B Pouvoirs de contrôle de la préposée cantonale ou du préposé cantonal en matière de protection des données personnelles (nouveau)

[1] La préposée cantonale ou le préposé cantonal peut effectuer, d'office, ou sur dénonciation, un contrôle auprès d'une institution ou d'un sous-traitant, afin de vérifier qu'ils respectent les dispositions de protection des données. Il décide librement des contrôles qu'il opère et de la suite à donner à une dénonciation.

[2] La préposée cantonale ou le préposé cantonal peut notamment demander des renseignements, exiger la production de documents, procéder à des inspections et se faire présenter des traitements de données. Elle ou il peut recourir, au besoin, à des experts dans les domaines techniques.

[3] Le secret de fonction ne peut pas être opposé à la préposée cantonale ou au préposé cantonal. Les autres secrets institués par la loi sont réservés.

[4] Si la personne concernée est à l'origine de la dénonciation, la préposée cantonale ou le préposé cantonal l'informe des suites données à celle-ci.

Art. 56C Mesures administratives de la préposée cantonale ou du préposé cantonal (nouveau)

[1] Si des dispositions de protection des données ne sont pas respectées, la préposée cantonale ou le préposé cantonal peut ordonner la modification, la

suspension ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction de tout ou partie des données personnelles.

[2] Elle ou il peut suspendre ou interdire la communication de données personnelles à l'étranger si elle est contraire aux conditions de l'article 39 ou à des dispositions d'autres lois cantonales concernant la communication de données personnelles à l'étranger.

[3] Elle ou il peut notamment ordonner à l'institution de:

a) se conformer à son devoir d'informer lors de la collecte des données (article 38);
b) répondre de manière appropriée à la demande de la personne concernée qui exerce ses droits en vertu de la présente loi, notamment son droit d'accès, son droit de rectification ou son droit d'opposition;
c) lui fournir les informations prévues en matière de communications transfrontières de données (article 38, alinéa 3);
d) déclarer un traitement de données personnelles au registre des activités des traitements (article 43);
e) prendre des mesures organisationnelles et techniques en matière de protection des données (article 37A);
f) prendre des mesures de protection des données dès la conception et par défaut (article 37);
g) procéder à une analyse d'impact relative à la protection des données personnelles ou la compléter (article 37B);
h) lui transmettre les informations pertinentes en lien avec une violation de la sécurité des données (article 37C);
i) informer les personnes concernées à la suite d'une violation de la sécurité des données (article 37C);
j) désigner une conseillère ou un conseiller LIPAD (article 50).

Art. 56D Procédure (nouveau)

[1] La procédure est régie par la loi sur la procédure administrative, du 12 septembre 1985.

[2] L'institution visée par une décision de la préposée cantonale ou du préposé cantonal a qualité pour recourir contre celle-ci.

Art. 56E Collaboration entre les autorités cantonales, fédérales et étrangères chargées de la protection des données (nouveau)

[1] Dans l'exercice de ses fonctions, la préposée cantonale ou le préposé cantonal doit collaborer avec les autorités cantonales, fédérales et étrangères chargées de la protection des données.

[2] La communication de données personnelles dans le cadre de l'entraide administrative est accordée lorsque les conditions fixées par l'article 39 de la présente loi sont remplies.

Art. 60 Recours en matière d'accès aux documents (nouvelle teneur de la note), al. 1 (nouvelle teneur), al. 2 (nouvelle teneur)

[1] En matière d'accès aux documents, seule est sujette à recours la décision que l'institution concernée prend à la suite de la recommandation formulée par la préposée cantonale ou le préposé cantonal en cas d'échec de la médiation. Les déterminations et autres mesures émanant des institutions en cette matière sont réputées ne pas constituer des décisions.

[2] Le recours contre les décisions que la Cour de justice prend en matière d'accès à ses propres documents à la suite de la recommandation de la préposée cantonale ou du préposé cantonal est du ressort de la Cour d'appel du pouvoir judiciaire.

Art. 68, al. 8 (nouveau)

Modifications du … (à compléter)

[8] Les articles 37 et 37B ne sont pas applicables aux traitements qui ont débuté avant l'entrée en vigueur de la loi XXX, du XXX, pour autant que les finalités du traitement restent inchangées et que de nouvelles données ne soient pas collectées.

Art. 2 Modifications à d'autres lois

[1] La loi sur la Haute école spécialisée de Suisse occidentale - Genève, du 29 août 2013 (LHES-SO-GE ; C 1 26), est modifiée comme suit :

Art. 6A Traitement de données personnelles (nouveau)

[1] La HES-SO Genève est en droit de traiter, à des fins de recherche, des données personnelles, y compris sensibles, et de procéder à du profilage, dans la mesure nécessaire à la réalisation de sa mission de recherche scientifique fondamentale et appliquée.

[2] Les dispositions de la loi fédérale relative à la recherche sur l'être humain, du 30 septembre 2011 et de la loi cantonale sur l'information du public, l'accès aux documents et à la protection des données personnelles, du 5 octobre 2001, ainsi que celles de leurs réglementations d'application respectives, demeurent réservées.

* * *

[2] La loi sur l'Université, du 13 juin 2008 (LU ; C 1 30), est modifiée comme suit :

Art. 7A Traitement de données personnelles (nouveau)

[1] L'université est en droit de traiter, à des fins de recherche, des données personnelles, y compris sensibles, et de procéder à du profilage, dans la mesure nécessaire à la réalisation de sa mission de recherche scientifique fondamentale et appliquée.

[2] Les dispositions de la loi fédérale relative à la recherche sur l'être humain, du 30 septembre 2011, et de la loi cantonale sur l'information du public, l'accès aux documents et à la protection des données personnelles, du 5 octobre 2001, ainsi que celles de leurs règlementations d'application respectives, demeurent réservées.

* * *

[3] La loi sur la surveillance de l'Etat, du 13 mars 2014 (LSurv ; D 1 09), est modifiée comme suit :

Art. 34 (nouvelle teneur)

Le rapport de révision des états financiers individuels et consolidés de l'Etat de Genève contient l'opinion du réviseur au sens de l'article 31 et recommande l'approbation des états financiers avec ou sans réserves, ou leur renvoi au Conseil d'Etat. Il est joint aux états financiers publiés et approuvés par le Conseil d'Etat. Les communications écrites complémentaires ne peuvent pas faire l'objet d'une demande d'accès aux documents au sens de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001. Il en va de même s'agissant des documents relatifs à d'autres entités reçus par la Cour des comptes dans le cadre de la révision des états financiers individuels et consolidés de l'Etat de Genève.

* * *

[4] La loi sur les établissements publics médicaux, du 19 septembre 1980 (LEPM; K 2 05), est modifiée comme suit :

Article 4A Traitement de données personnelles (nouveau)

[1] Les Hôpitaux universitaires de Genève sont en droit de traiter, à des fins de recherche, des données personnelles, y compris sensibles, et de procéder à du profilage, dans la mesure nécessaire à la réalisation de leur mission de recherche médicale fondamentale et clinique.

[2] Les dispositions de la loi fédérale relative à la recherche sur l'être humain, du 30 septembre 2011 et de la loi cantonale sur l'information du public, l'accès aux documents et à la protection des données personnelles, du 5 octobre 2001, ainsi que celles de leurs réglementations d'application respectives, demeurent réservées.

* * *

Art. 3 Entrée en vigueur

Le Conseil d'Etat fixe la date d'entrée en vigueur de la présente loi.

Certifié conforme
La chancelière d'Etat : Michèle RIGHETTI

EXPOSÉ DES MOTIFS

Mesdames et
Messieurs les Députés,

I. Introduction

Faisant œuvre de pionnier, le législateur genevois s'est préoccupé d'assurer la protection de certaines données personnelles dès l'émergence des nouvelles technologies de l'information, en adoptant, le 24 juin 1976 déjà, une loi sur la protection des informations traitées automatiquement par ordinateur, puis, le 17 décembre 1981, une nouvelle loi sur les informations traitées automatiquement par ordinateur (LITAO)[1].

La loi genevoise sur l'information du public et l'accès aux documents a été adoptée le 5 octobre 2001 et est entrée en vigueur le 1er mars 2002[2]. Suite à une révision importante, adoptée le 9 octobre 2008 et entrée en vigueur le 1er janvier 2010, le domaine de la protection des données personnelles s'est ajouté au volet de la transparence. La loi sur l'information du public et l'accès aux documents est ainsi devenue la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (ci-après « LIPAD »).

Depuis lors, de nombreuses évolutions ont eu lieu, d'un point de vue tant technologique, sociétal, que juridique. Le présent projet de loi vise à adapter la LIPAD à ces développements, et notamment aux réformes du Conseil de l'Europe et de l'Union européenne en matière de protection des données, et à la révision du droit fédéral qui en découle.

II. Contexte juridique international

CEDH

La Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (CEDH; RS 0.101), conclue à Rome le 4 novembre 1950 et entrée en vigueur pour la Suisse le 28 novembre 1974, prévoit à son art. 8 que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

[1] PL 9870, p. 30
[2] A 2 08

Conseil de l'Europe

Le Conseil de l'Europe a adopté, le 28 janvier 1981, le premier traité international en matière de protection des données, à savoir la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après *« convention STE 108 »*)[3], qui a été ratifiée par la Suisse le 2 octobre 1997. Cette convention a été complétée par le protocole additionnel du 8 novembre 2001 à la convention STE 108 concernant les autorités de contrôle et les flux transfrontières de données[4] (STE 181 ; ci-après *« protocole additionnel »*) que la Suisse a également ratifié, le 20 décembre 2007.

En 2011, le Conseil de l'Europe a entamé une procédure de modernisation de la convention STE 108 et de son protocole additionnel dans l'objectif 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 des droits fondamentaux des personnes concernées. Les travaux ont été menés en parallèle avec la réforme du cadre législatif en matière de protection des données de l'Union européenne (UE) et la plus grande attention a été portée au maintien de la cohérence entre les deux cadres législatifs. Le cadre de l'UE en matière de protection des données précise et amplifie les principes de la Convention 108 et prend en considération l'adhésion à la Convention, notamment au regard des transferts internationaux.

La 128ème session ministérielle du Comité des Ministres du Conseil de l'Europe a adopté l'amendement (STCE n°223) à la Convention pour la protection des personnes à l'égard du traitement automatisé des données personnelles (STE n°108) le 18 mai 2018 et a entériné son Rapport explicatif. Cette modernisation vise à harmoniser et renforcer le niveau de protection des données au plan international, avec pour effet de renforcer aussi la protection dont bénéficient les citoyens suisses lorsque leurs données personnelles font l'objet de traitements transfrontières. Cette modernisation a également pour but de faciliter les flux transfrontières de données entre les

[3] RS 0.235.1
[4] RS 0.235.11

Etats parties, permettant ainsi un accès facilité au marché de ces pays pour les entreprises suisses[5].

Le Protocole a été ouvert à la signature le 10 octobre 2018. Dans un communiqué daté du 30 octobre 2019, le Conseil fédéral a annoncé l'avoir signé. Lors de sa séance du 6 décembre 2019, il a adopté le message relatif à l'approbation du Protocole[6]. L'arrêté fédéral portant approbation du Protocole a été approuvé le 19 juin 2020 par l'Assemblée fédérale[7]. Il n'y a pas eu de référendum.

L'approbation du Protocole par la Suisse lie également les cantons. Les dispositions de cet acte (ci-après *« Convention 108+ »*) doivent être transposées, si besoin est, conformément à la répartition constitutionnelle des compétentes prévues en droit interne[8].

Union européenne

L'Union européenne (UE) a adopté, ces dernières décennies, plusieurs textes législatifs en vue de protéger les données à caractère personnel.

Le texte principal est la directive 95/46/CE du 24 octobre 1995[9] 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 (ci-après la *« directive 95/46/CE »*). Celle-ci a été complétée par la décision-cadre 2008/977/JAI[10] du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Le 27 avril 2016, le Parlement européen et le Conseil de l'Union européenne ont adopté une réforme de la législation sur la protection des données qui comprend deux actes législatif, soit :

[5] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, du 15 septembre 2017 (ci-après « Message »), FF 2017 6565, p. 6617
[6] FF 2020 545-574
[7] FF 2020 5559 s
[8] Message, p. 237
[9] JO L 281 du 23.11.1995, p. 31
[10] JO L 350 du 30.12.2008, p. 60

- le règlement (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après *« RGPD »*)[11] ; et
- la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (ci-après *« directive (UE) 2016/680 »*)[12].

Le RGPD est le texte fondamental en matière de protection des données au niveau de l'Union européenne. Il a remplacé la directive 95/46/CE au sein de l'Union européenne. La directive (UE) 2016/680 s'en inspire largement, au point que les deux textes contiennent un régime très analogue. Le règlement est cependant plus détaillé, et la directive contient des particularités propres au domaine pénal[13].

La directive (UE) 2016/680 vise à protéger les données à caractère personnel traitées 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cet acte a pour objectif de garantir un niveau élevé de protection des données des personnes physiques tout en facilitant l'échange de ces données entre les autorités compétentes des différents Etats Schengen[14].

La directive (UE) 2016/680 constitue pour la Suisse un développement de l'acquis de Schengen; celle-ci doit donc le reprendre en vertu de l'accord

[11] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016 p.1

[12] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016 p. 89

[13] Message, FF 2017 6565, p. 6618

[14] Message, FF 2017 6565, p. 6611

d'association à Schengen. Cela vaut également pour les cantons[15]. En revanche, la Suisse n'est pas tenue de reprendre le RGPD car, selon l'Union européenne, il ne constitue pas un développement de l'acquis de Schengen[16].

Décision d'adéquation

Dans les domaines qui ne relèvent pas de la coopération instaurée par Schengen et Dublin, la Suisse est considérée comme un Etat tiers. Or, l'échange de données entre un Etat tiers et les Etats membres de l'Union européenne ne peut se faire que si le pays tiers assure un niveau de protection adéquat au sens de la directive 95/46/CE. Ce niveau de protection fait régulièrement l'objet d'une évaluation de la Commission européenne, qui rend, le cas échéant, une décision d'adéquation. Cette dernière peut être révoquée en tout temps[17].

Par décision du 26 juillet 2000, la Commission européenne a constaté que la Suisse dispose d'un niveau de protection adéquat des données[18]. Cette décision se fonde toutefois sur le niveau de protection défini par la directive 95/46/CE. L'Union européenne procèdera prochainement à une nouvelle évaluation du droit suisse afin de vérifier sa compatibilité avec le RGPD. Dans le cadre de cette évaluation, elle examinera le droit fédéral, mais aussi le droit de certains cantons choisis de manière aléatoire.

Recommandations suite à l'évaluation Schengen

En s'associant à Schengen-Dublin, la Suisse s'est engagée à ce que les traitements de données personnelles effectués dans le cadre de la coopération Schengen soient conformes à la réglementation de l'Union européenne applicable en matière de protection des données.

La dernière évaluation a eu lieu en 2018. Une des recommandations faites à la Suisse a cette occasion a été de renforcer les pouvoirs d'exécution des

[15] Message, FF 2017 6565, p. 6628
[16] Message, FF 2017 6565, p. 6587
[17] Message, FF 2017 6565, p. 6588
[18] Décision de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse, JO L 215 du 25.8.2000, p. 1

autorités cantonales chargées de la protection des données en les habilitant à prendre directement des décisions juridiquement contraignantes[19].

La prochaine évaluation aura lieu en 2023[20].

III. Contexte juridique national

Lors de sa séance du 21 décembre 2016, le Conseil fédéral a mis en consultation un avant-projet de révision totale de la loi fédérale sur la protection des données du 19 juin 1992 (LPD; RS 235.1). Le projet visait à réaliser deux objectifs principaux : renforcer les dispositions légales de protection des données pour faire face au développement fulgurant des nouvelles technologies d'une part et, d'autre part, tenir compte des réformes du Conseil de l'Europe et de l'Union européenne en la matière, afin de rendre la législation fédérale compatible avec la Convention 108+ et à mettre en œuvre les exigences de la directive (UE) 2016/680, conformément aux engagements pris par la Suisse dans le cadre de l'Accord d'association à Schengen. En outre, le projet doit permettre de rapprocher le droit fédéral des exigences du RGPD. Ce rapprochement, ainsi que l'approbation de la Convention modernisée, constituent des conditions déterminantes pour que la Commission européenne maintienne la décision d'adéquation accordée à la Suisse[21].

Le 11 janvier 2018, la Commission des institutions politiques du Conseil national (CIP-N) est entrée en matière sans opposition sur le projet du Conseil fédéral concernant ce projet de révision totale. Parallèlement, elle a adopté une motion d'ordre demandant la scission du projet. Elle a souhaité de la sorte échelonner la révision prévue : dans un premier temps, la Commission a examiné la mise en œuvre du droit européen (directive (UE) 2016/680) qui, en vertu des Accords de Schengen, devait avoir lieu dans un délai donné, avant de s'atteler ensuite à l'examen de la révision totale de la LPD sans être contrainte par le temps.

Suite à cette décision, le Parlement a adopté, le 28 septembre 2018, la loi fédérale sur la protection des données personnelles dans le cadre de

[19] Décision d'exécution du Conseil de l'Union européenne 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, du 8 mars 2019

[20] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-75749.html

[21] Message, FF 2017 6565, p. 6567

l'application de l'acquis de Schengen dans le domaine pénal (Loi sur la protection des données Schengen, LPDS ; RS 235.3).

Le 25 septembre 2020, la nouvelle LPD a été acceptée par les deux chambres[22] (ci-après *« nLPD »*). Lors de l'entrée en vigueur du texte, la LPDS sera abrogée, au motif que les dispositions de cette loi feront double emploi avec celles de la nLPD. Elle devrait en principe entrer en vigueur durant le second semestre 2022.

IV. Grands traits du présent projet

Le présent projet s'inspire en grande partie de la nLPD, dans la mesure où cette dernière s'inspire elle-même des nouveaux textes de la troisième génération de législation en matière de protection des données que sont la Convention 108+, la Directive (UE) 680/2016 et le RGPD.

A l'instar de ces règlementations, le présent 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 du traitement dont les activités présentent un risque accru d'atteinte que pour ceux dont les activités sont moins risquées[23] ;
- à l'instar de la nLPD, le présent projet traite dans la mesure du possible de manière égale les différentes technologies - la loi peut ainsi s'adapter aux évolutions technologiques sans freiner l'innovation ;
- À l'instar de la nLPD, la terminologie utilisée dans la LIPAD actuellement en vigueur a été modernisée - cela a notamment pour objectif d'améliorer la compatibilité du droit suisse avec le droit de l'Union européenne ; la notion de *« maître du fichier »* est ainsi remplacée par celle de *« responsable du traitement »* (voir *supra* commentaire ad art. 4). La notion de *« profil de la personnalité »* qui constitue une particularité suisse, disparaît au profit de la notion de *« profilage »* (voir *supra* ad art. 4). La notion de « données sensibles » est étendue aux *« données génétiques »* et aux *« données biométriques »* (voir *supra* commentaire ad art. 4).

[22] FF 2020 7397 ss
[23] FF 2017 6565, p. 6593

A. Champ d'application de la LIPAD

Pas de modification pour les personnes morales

Les textes de protection des données de l'Union européenne et du Conseil de l'Europe ainsi que ceux de la majorité des pays étrangers ne prévoient pas de protection des données personnelles des personnes morales.

La Confédération a ainsi décidé de supprimer la protection desdites données de la nLPD. Toutefois, 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[24]. 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[25]. 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. Il a procédé au même exercice avec la législation spéciale où les règles qui autorisent le traitement des données personnelles ont été doublées pour autoriser aussi le traitement des données de personnes morales.

Or, la suppression de la protection des données personnelles des personnes morales de la LIPAD conduirait à un vide juridique, qui devrait être comblé dans d'autres textes légaux, à l'instar de ce qui a été fait au niveau fédéral. Dans la mesure où le droit supérieur n'impose rien à ce sujet, et que la LIPAD dans sa teneur actuelle a donné satisfaction jusqu'à présent sur ce point, le Conseil d'Etat propose de maintenir le statu quo sur ce point.

Inclusion de la Cour des comptes

La question de l'inclusion ou non de la Cour des comptes dans le champ d'application de la LIPAD a été soulevée à de nombreuses reprises ces

[24] FF 2017 6565, p. 6595, 6603ss et 6633
[25] FF 2017 6565, p. 6722 et 6733

derniers temps sans qu'une réponse claire ne puisse y être apportée[26]. Cette incertitude juridique est notamment renforcée par la mention de la Cour des comptes à l'actuel article 41, alinéa 2 LIPAD relatif au traitement des données personnelles à des fins générales (de statistique, de recherche scientifique, de planification ou d'évaluation de politiques publiques) qui réserve les compétences et les règles de fonctionnement de la Cour des comptes dans le cadre de cette disposition.

Pour sa part, la Cour des comptes a émis des doutes sur sa soumission au champ d'application de la LIPAD, principalement puisqu'elle ne figurait pas expressément dans la liste des institutions soumises à ladite loi prévue à son article 3. Sur une base volontaire, elle en a toutefois toujours appliqué les principes s'agissant du volet relatif à la protection des données personnelles dans le cadre de ses activités légales et elle a participé volontairement à un processus de médiation à propos de la publication partielle de l'un de ses rapports.

Le Conseil d'Etat vous propose ainsi d'inclure formellement la Cour des comptes dans le champ d'application de la LIPAD, dans un but de clarté et afin de lever toute ambiguïté. Le projet de modifications porte sur les articles 3, alinéa 1, lettre c, 13A et 20A (nouvelle section 5) et 26, alinéa. 2 lettre d, ainsi que l'article 34 LSurv (voir *infra* commentaire article par article pour plus de détails).

Inclusion des personnes physiques et morales ou des organismes chargés de remplir des tâches publiques dans les entités soumises au volet de la protection des données

Actuellement, l'article 3, alinéa 2, lettre b LIPAD soumet au champ de la loi, mais tout en réservant les alinéas 4 et 5, les personnes physiques et morales ou les organismes chargés de remplir des tâches de droit public cantonal ou communal, dans les limites de l'accomplissement desdites tâches.

Dans le projet qui vous est soumis, il est proposé de supprimer la teneur de l'article 3, alinéa 4 LIPAD qui prévoit que le traitement de données personnelles par une personne physique et morale de droit privé n'est pas soumis à la présente loi. Cette suppression entraîne l'application de la loi aux

[26] Voir à ce titre l'ATA/831/2020 et le commentaire du préposé cantonal et de la préposée cantonale adjointe du 21 décembre 2020 *in* swissprivacy.law, https://swissprivacy.law/44/

entités de droit privé chargées de remplir des tâches publiques. Il est également proposé de déplacer l'article 3, alinéa 2, lettre b LIPAD à l'alinéa 1, parmi les entités auxquels tant le volet transparence que le volet protection des données personnel sont applicables.

En effet, si, conformément à la force dérogatoire du droit fédéral, une personne physique ou morale de droit privé est d'office soumise au champ d'application de la loi fédérale sur la protection des données, il n'est toutefois pas exclu qu'elle puisse être soumise à des règles cantonales lorsqu'elle accomplit des tâches de droit cantonal ou communal. Lorsque des personnes physiques ou morales et organismes sont chargés de remplir des tâches de droit public cantonal ou communal, au sens de l'article 3, alinéa 2, lettre b LIPAD, il faut considérer qu'elles agissent en tant qu'organes de l'Etat et qu'en tant que telles, elles sont soumises à la LIPAD dans les limites de l'accomplissement desdites tâches. Il paraît en effet difficilement justifiable que l'Etat puisse s'affranchir du respect du droit cantonal en matière de protection des données lorsqu'il recourt à des tiers externes à l'administration pour l'accomplissement de tâches publiques. C'est ce qui est d'ailleurs prévu dans d'autres législations cantonales et dans la nLPD[27].

Exclusion des traitements de données personnelles effectués par la Banque cantonale de Genève

A l'instar de plusieurs cantons possédant une banque cantonale, le présent projet propose à l'article 3, alinéa 4 d'exclure du champ d'application de la loi cantonale les traitements de données personnelles effectués par la Banque cantonale de Genève. Celle-ci est une société anonyme de droit public au sens de l'art. 763 CO, dont les activités sont essentiellement régies par les lois fédérales sur les banques, les bourses et le commerce de valeurs mobilières, et ses relations avec sa clientèle et avec son personnel sont régies par le droit privé. Il s'ensuit que ses traitements de données personnelles doivent être soumis à la loi fédérale sur la protection des données, qui régit notamment les traitements de données personnelles effectués par des personnes privées, et non pas à la loi cantonale.

[27] C'est ce qui est notamment prévu dans les cantons de Vaud, Fribourg, Jura, Neuchâtel, Valais, Berne, et Zurich. Voir également article 5, let. i nLPD, qui définit l'organe fédéral comme l'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération;

B. Autres modifications

Introduction du consentement comme motif justificatif extra-légal

A l'instar de la nLPD, le présent projet introduit le consentement de la personne concernée comme motif pouvant justifier un traitement de données personnelles, y compris sensibles (voir *infra* commentaire ad art. 36A).

Inclusion de la notion de sous-traitance dans la loi

La notion de sous-traitance, figurant à l'heure actuelle dans le règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 21 décembre 2011 (RIPAD ; A 2 08.01) (voir *infra* commentaire ad art. 36C), est ancrée au niveau de la loi.

Renforcement des obligations des responsables du traitement

Le présent projet inclut les notions de protection des données dès la conception (en anglais : *« privacy by design »*) et par défaut (en anglais : *« privacy by default »*) (voir *infra* commentaire ad art. 37). La première signifie que le responsable du traitement doit mettre en place des mesures techniques et organisationnelles 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. La deuxième implique que le responsable du traitement est tenu, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

Par ailleurs, le présent projet prévoit qu'avant de débuter un nouveau traitement de données qui est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, le responsable du traitement est tenu d'accomplir préalablement une analyse d'impact relative à la protection des données (voir *infra* commentaire ad art. 37B). Il s'agit d'un instrument destiné à identifier et à évaluer les risques que certains traitements de données personnelles pourraient entraîner pour la personne concernée. Le cas échéant, cette analyse doit servir à définir des mesures pour faire face à ces risques. L'avantage pour le responsable du traitement est qu'elle permet d'anticiper d'éventuels problèmes juridiques liés à la protection des données et d'éviter les coûts qui pourraient en résulter[28].

[28] FF 2017 6565, p. 6676

Enfin, en cas de violation de la protection des données, le responsable du traitement doit prendre immédiatement les mesures appropriées afin de mettre fin à la violation et d'en minimiser les effets et doit annoncer la violation dans les meilleurs délais à la préposée cantonale au préposé cantonal et, dans les cas les plus graves, directement à la personne concernée (voir *infra* commentaire ad art. 37C).

Renforcement de la transparence des traitements de données et de la maîtrise par les personnes concernées sur leurs données

Le projet définit plus en détail l'obligation d'informer les personnes concernées et la liste d'informations à fournir à ces dernières (voir *infra* commentaire ad art. 38). Les droits des personnes concernées sont également clarifiés. Entre autres, le projet mentionne expressément le droit à l'effacement des données, ainsi que des moyens de défenses spécifiques 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 être informée qu'il s'agit d'une décision rendue exclusivement sur la base d'un traitement de données personnelles automatisé (i.e. 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 former une réclamation gratuite à l'encontre de la décision en question (voir *infra* commentaire ad art. 38B).

Adaptation des règles relatives aux traitements de données personnelles à des fins générales de statistique, de recherche scientifique, de planification ou d'évaluation de politiques publiques

Le présent projet adapte la disposition relative aux traitements de données personnelles, y compris sensibles, à des fins générales de statistique, de recherche scientifique, de planification ou d'évaluation de politiques publiques afin de la calquer sur la disposition *ad hoc* de la nLPD à des fins de cohérence et pour en faciliter l'application (voir *infra* commentaire ad art. 41).

Renforcement des missions et compétences de la préposée cantonale ou du préposé cantonal

Le présent projet prévoit le renforcement du rôle et des pouvoirs de la préposée cantonale ou du préposé cantonal, comparables à ceux des autorités de contrôle des autres pays européens. Le projet renforce les pouvoirs de

contrôle de la préposée cantonale ou du préposé cantonal (voir *infra* commentaire ad art. 56B) et prévoit que cette dernière ou ce dernier, à l'instar de ses homologues européens, peut prendre des décisions contraignantes à l'égard des responsables du traitement. A l'instar de ce qui a été prévu dans la nLPD pour les organes fédéraux, il n'est toutefois pas habilité à prononcer des sanctions administratives, cette notion faisant peu de sens dans la mesure où la LIPAD, dans son volet protection des données, ne s'applique qu'à des institutions[29] ou à des entités de droit privé dans l'accomplissement de tâches de droit public (voir *infra* commentaire ad art. 56C).

V. Commentaire article par article du projet de loi modifiant la LIPAD

Art. 3

Al. 1

Cet alinéa a été modifié pour introduire la Cour des comptes, comme indiqué plus haut, dans la liste des institutions soumises à la LIPAD. Il a également été complété par l'inclusion des personnes physiques et morales ou organismes chargés d'accomplir des tâches publiques cantonales ou communales, dans les limites de l'accomplissement desdites tâches.

Al. 2

Quant à l'alinéa 2, il ne concernera désormais plus que les entités maîtrisées effectivement par les institutions mentionnées à l'alinéa 1, les personnes physiques ou morales et organismes chargés de remplir des tâches de droit public cantonal ou communal ayant été déplacés à l'alinéa 1. Compte tenu de la suppression de la teneur de l'article 3, alinéa 4 LIPAD, la réserve à l'alinéa 4 a été supprimée et remplacée, à des fins didactiques, par une mention explicite de la non application du Titre III relatif à la protection des données personnelles. Il s'agit en réalité de reformulation qui ne modifie pas la situation matérielle de ces entités qui, déjà actuellement, ne sont soumises qu'au volet *« transparence »* de la LIPAD.

Al. 4

[29] FF 2017 6565, p. 6589

Comme indiqué plus haut, il semblait opportun de soumettre les personnes physiques ou morales et les organismes chargés de remplir des tâches de droit public cantonal ou communal au sens de l'article 3, alinéa 2, lettre b (teneur actuelle) LIPAD - dans les limites de l'accomplissement desdites tâches – aux dispositions cantonales de protection des données plutôt qu'à la loi fédérale sur la protection des données, qui s'applique aux organes fédéraux et aux personnes privées.

Par ailleurs, les autres entités de droit privé sont automatiquement soumises à la loi fédérale. A des fins didactiques, une exclusion de l'application du Titre III a été précisée à l'alinéa 2.

Enfin, comme expliqué plus haut (voir *supra* Chapitre IV.A), la nouvelle teneur de l'alinéa 4 exclut les traitements de données personnelles effectués par la Banque cantonale de Genève (BCGE), en raison de son activité de droit privé, régie par le droit fédéral.

Art. 4

De manière générale, les définitions ont été adaptées en s'inspirant le plus possible de celles retenues par la nLPD, en vue de faciliter les futures interprétations par les autorités d'application.

Les opinions et les activités culturelles ne font désormais plus parties des données personnelles sensibles, dans la mesure où cette notion n'est prévue dans aucun autre texte, suisse ou européen.

S'agissant de la notion des données personnelles sensibles, les termes *« appartenance ethnique »* sont remplacés par *« origine raciale ou ethnique »*, conformément à la Convention 108+[30], la directive (UE) 2016/680[31] et la nLPD[32]. Le RGPD prévoit une règlementation identique[33].

La notion de données personnelles sensibles est désormais par ailleurs élargie, à l'article 4, lettre b, aux *« données génétiques »* et aux *« données biométriques »*. Cette modification transpose les exigences de la Convention 108+[34] et de la directive (UE) 2016/680[35], et est conforme à la nLPD[36]. Le RGPD prévoit une règlementation identique[37].

[30] Art. 6, par. 1
[31] Art. 10
[32] Art. 5, let. c, ch. 2
[33] Art. 9
[34] Art. 6, par. 1
[35] Art. 10

Les *« données génétiques »* sont toutes les données relatives aux caractéristiques héréditaires d'un individu ou acquises à un stade précoce du développement prénatal, résultant de l'analyse d'un échantillon biologique de cet individu : analyse des chromosomes, de l'ADN ou de l'ARN, ou de tout autre élément permettant d'obtenir des informations équivalentes[38].

Par *« données biométriques »*, on entend les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne, qui résultent d'un traitement technique spécifique et permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images faciales, de l'iris, ou encore de la voix. Ces données doivent impérativement résulter d'un traitement technique spécifique qui permet l'identification ou l'authentification unique d'un individu. Tel ne sera en principe pas le cas, par exemple, de simples photographies[39]. A noter que le Conseil d'Etat propose de s'aligner sur la Convention 108+[40], la directive (UE) 2016/680[41] et le RGPD[42], qui utilisent tous trois le terme *« unique »* (et non *« univoque »* comme cela figure dans la nLPD).

Le présent projet conserve la référence aux données relatives à la santé et à la sphère intime, à l'instar de la nLPD[43]. Constituent notamment des données relatives à la sphère intime les données concernant la vie sexuelle et l'orientation sexuelle de la personne concernée[44].

A l'instar de la nLPD[45], la notion de *« profil de personnalité »* est remplacé par celle de *« profilage »*, que l'on retrouve également dans la directive (UE) 2016/680[46] et le RGPD[47]. En effet, ces deux notions, bien que présentant de nombreuses similitudes, ne couvrent pas le même état de fait. Le profil de la personnalité est le résultat d'un traitement et traduit ainsi quelque chose de statique. A l'inverse, le profilage se définit ainsi comme

[36] Art. 5, let. c, ch. 3 et 4
[37] Art. 4, par. 13 et 14
[38] Rapport explicatif de la Convention 108 modernisée, ch. 57 ad art. 6
[39] FF 2017 6565, p. 6641
[40] Art. 6, par. 1
[41] Art. 3, ch. 13
[42] Art. 9, par. 1
[43] Art. 5, let. c, ch. 2
[44] FF 2017 6565, p. 6640; voir aussi l'article 6, par. 1 de la Convention 108+, l'article 10 de la directive (UE) 2016/680 et l'article 9 RGPD
[45] Art. 5, let. f
[46] Art. 3, ch. 4
[47] Art. 4, ch. 4

l'évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée afin notamment d'analyser ou de prédire son rendement au travail, sa situation économique, sa localisation, sa santé, son comportement, ses préférences ou ses déplacements. L'analyse de ces caractéristiques peut par exemple avoir pour but de déterminer si une personne est indiquée pour une certaine activité. Autrement dit, le profilage se caractérise par le fait qu'on procède à une évaluation automatisée de données personnelles afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne. On est ainsi en présence d'un profilage uniquement lorsque le processus d'évaluation est entièrement automatisé[48]. Même si l'évaluation de la machine est basée sur une commande humaine, elle se fait toujours de manière schématique. Pour qu'un processus soit considéré comme un profilage, il faut que le profilage soit la finalité ou le motif du traitement des données. Par exemple, si un marchand de vins établit des statistiques sur les types de vins achetés par ses clients afin de mieux concevoir son assortiment, il ne s'agit pas d'un profilage. Si, en revanche, à partir de la même base de données, il établit une liste de tous les acheteurs de vins espagnols dans le but de leur écrire parce qu'il pense qu'ils seront les plus à même d'être intéressés par une nouvelle livraison de ces vins (évaluation automatique), il s'agit d'un profilage. S'il sélectionne chaque client manuellement, ce n'est plus un profilage. En effet, à l'instar de la directive (UE) 2016/680 et du RGPD, la LPD ne prévoit pas de profilage manuel[49].

La définition de traitement a été légèrement modifiée, pour s'étendre à *« l'effacement »*, *« l'interconnexion »* et le *« rapprochement »*, dans le but de se rapprocher des textes européens[50]. La liste des opérations entrant en ligne de compte dans la définition du *« traitement »* n'est pas exhaustive, les opérations de traitement pouvant prendre les formes les plus diverses.

L'*« interconnexion »* et le *« rapprochement »* sont des notions proches mais différentes. Conformément aux critères posés par la CNIL (Commission nationale française de l'informatique et des libertés), l'objet de l'interconnexion doit être la mise en relation de fichiers ou de traitements de données personnelles. En second lieu, cette mise en relation doit concerner au moins deux fichiers ou traitements distincts. Enfin, l'interconnexion doit consister en un processus automatisé ayant pour objet de mettre en relation des informations issues des fichiers ou traitements. Le rapprochement, tout

[48] FF 2017 6565, p. 6642
[49] ROSENTHAL, op. cit., ch. 26
[50] Voir art. 3, par. 2 de la directive (UE) 2016/680 et art. 4, par 2 RGPD

comme l'interconnexion, constitue une mise en relation d'informations. Cependant, le rapprochement se distingue de l'interconnexion sur deux points. A la différence d'une interconnexion, un rapprochement ne suppose pas nécessairement la mise en œuvre de moyens automatisés. Ainsi, la comparaison visuelle d'informations issues de deux fichiers ou encore l'enrichissement d'un fichier existant par saisie manuelle d'informations issues d'un autre fichier ne constituent pas une interconnexion, mais de simples rapprochements. Un rapprochement peut être réalisé au sein d'un même traitement ou fichier, alors qu'une interconnexion implique deux fichiers distincts[51].

Les définitions du *« caviardage »*, de l'*« anonymisation »* et de la *« pseudonymisation »* ont été ajoutées, pour une meilleure compréhension de ces notions. Le terme d'*« anonymisation »* vise ainsi tout traitement de données personnelles consistant à supprimer définitivement toutes les données identifiantes ou tout moyen de retrouver les données originales. L'anonymisation se distingue de la pseudonymisation en ce sens qu'est irréversible, contrairement à la pseudonymisation (voir ci-après). A noter que des données parfaitement anonymisées ne sont plus considérées comme des données personnelles, dans la mesure où elles ne permettent plus d'identifier une personne physique ou morale. La *« pseudonymisation »* vise quant à elle tout traitement de données personnelles consistant à remplacer l'ensemble des données identifiantes par un identifiant neutre (pseudonyme), de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires. Les données identifiantes doivent être conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable. Comme indiqué plus haut, contrairement à l'anonymisation, la pseudonymisation est réversible (tant qu'une table de correspondance permettant de faire le lien entre le pseudonyme et les données identifiantes d'une personne existe et est accessible). Enfin, le *« caviardage »* consiste, dans un traitement de données personnelles, à masquer des passages ou des données d'un document en vue de sa communication ou de sa publication, de sorte que la personne physique ou morale concernée ne puisse pas être identifiée.

La notion de *« fichier »* est supprimée, à l'instar de ce qui est prévu pour la nLPD. Cela correspond à la solution retenue par la Convention 108+, qui recourt en lieu et place à la notion de « *traitement* ». En effet, compte tenu des nouvelles technologies, les données peuvent aujourd'hui être exploitées comme un fichier, alors même qu'elles sont disséminées. Un exemple parlant

[51] https://www.cnil.fr/en/node/15316

est le profilage, lors duquel on va chercher des données dans différentes sources, non constitutives de fichiers, afin d'évaluer certaines caractéristiques d'une personne[52].

Le présent projet introduit les notions de *« responsables du traitement »* et de *« sous-traitant »*. Ces définitions s'inspirent de celles de la nLPD[53], ainsi que sur celles de la Convention 108+[54], de la directive (UE) 2016/680[55], et du RGPD[56]. Du fait de l'introduction de la notion de *« responsable du traitement »*, la définition d'organe a été supprimée de l'art. 4 et remplacée dans le corps de la loi.

Du fait de la suppression de la notion de fichier, le présent projet remplace également la notion de *« maître du fichier »* par celle de *« responsable du traitement »*. Le responsable du traitement est toute institution au sens de l'article 3 qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles. Cette définition s'inspire de celle de la nLPD[57] et vise à utiliser la même terminologie que celle de la Convention 108+[58], de la directive (UE) 2016/680[59] et du RGPD[60].

Le *« sous-traitant »*, quant à lui, est toute institution, organisme ou personne physique ou morale qui traite des données personnelles pour le compte du responsable du traitement. Cette définition s'inspire de celle de la nLPD[61] qui reprend celle de la Convention 108+[62].

Le présent projet introduit une définition de la *« sécurité des données »*, soit l'ensemble des mesures organisationnelles et techniques permettant d'assurer la confidentialité, l'intégrité et la disponibilité des données. Il introduit également, à l'instar de la nLPD[63], une définition de la *« violation de la sécurité des données »*. Est considérée comme telle toute violation de la

[52] FF 2017 6565, p. 6643
[53] Art. 5, let. k
[54] Art. 2, let. d et f
[55] Art. 3, par. 8 et 9
[56] Art. 4, par. 7 et 8
[57] Art. 5 let. j
[58] Art. 2 let. d
[59] Art. 3 par. 8
[60] Art. 4 par. 7
[61] Art. 5 let. k
[62] Art. 2 let. f ; voir également art. 3 par. 9 Directive (UE) 2016/680 et art. 4, par. 8 RGPD
[63] Art. 5, let. h

sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données. La directive (UE) 2016/679[64] et le RGPD[65] contiennent également une définition de cette notion.

Enfin, le présent projet introduit une nouvelle définition, celle de *« décision individuelle automatisée ».* Cette notion est en effet reprise plus loin dans le corps du projet, conformément aux nouvelles exigences du droit supérieur. Il s'agit de toute décision prise exclusivement sur la base d'un traitement de données automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

Section 4A, article 13A

La section 4A relative à la Cour des comptes est nouvelle. Elle fait partie du chapitre I relatif à la publicité des séances et est introduite, à l'instar de ce qui est prévu pour le Grand Conseil, le Conseil d'Etat, le Pouvoir judiciaire, les communes et les établissements et corporations de droit public, pour préciser la question de la publicité des séances en lien avec les délibérations et autres séances de la Cour des comptes. L'article 13A précise ainsi que ces dernières se tiennent à huis clos.

Art. 20A

Cet article fait partie du chapitre II de la loi relatif à l'information du public et vient préciser les modalités de cette dernière par la Cour des comptes.

La Cour des comptes mène déjà une politique active d'information du public par la diffusion de ses rapports, d'examens dits *« sommaires »* ou *« ciblés »*, d'une newsletter, de son rapport annuel et d'articles de ses collaboratrices et collaborateurs. Elle place sur son site les communiqués qu'elle adresse à la presse et les vidéos qu'elle produit, de même que les annexes méthodologiques, voire certains rapports produits par des mandataires. L'alinéa 1 formalise cette activité et précise ainsi que la Cour des comptes informe le public par le biais de la publication de ses rapports et d'autres documents qu'elle considère d'intérêt public. Il précise toutefois également que dans ce cadre, la Cour des comptes veille à la protection du

[64] Art. 3, par. 11
[65] Art. 4, par. 12

secret professionnel, de fonction, fiscal ou d'affaires des personnes entendues, et de toute autre secret prévu par la loi.

L'alinéa 2 prévoit quant à lui que la Cour des comptes ne peut donner d'informations au public susceptibles de permettre l'identification de l'auteur d'une communication ou d'une personne, sous réserve toutefois des règles qui régissent son activité.

Enfin, l'alinéa 3 précise que la Cour des comptes veille, dans le cadre de l'information du public, au respect des règles professionnelles prohibant la transmission d'informations ou la transmission de documents en matière d'audit, d'évaluation ou de révision. Les contours de la transparence pour ce qui concerne l'activité de révision des comptes de l'Etat qui incombe à la Cour des comptes sont traités par la modification à la loi sur la surveillance (voir également *infra*, modifications à d'autres lois, commentaire *ad* art. 34 LSurv.)

Art. 26, al. 2. let. d

Cette disposition a été complétée par le terme *« investigations »*, suite à l'introduction de la Cour des comptes parmi les institutions soumises à la LIPAD.

Art. 28, al. 3 et al. 4

Al. 3

Cet alinéa est nouveau et a été introduit pour régler les cas où plusieurs demandes d'accès portent sur un même document détenu par plusieurs institutions. Dans un tel cas, cet alinéa prévoit que lesdites institutions déterminent laquelle traite la demande, et en informent la requérante ou le requérant. Les autres demandes d'accès deviennent ainsi sans objet.

Al. 4

Cet alinéa (ancien alinéa 3) a été modifié pour refléter la modification de terminologie et le remplacement de la notion de *« responsable »* (au sens de l'art. 50 LIPAD) par celle de *« conseillère ou conseiller à la protection des données et à la transparence »* (voir également *infra* commentaire ad art. 50).

Art. 30, al. 5

Cet alinéa a été complété afin de prévoir, à l'instar de ce qui figure à l'article 49, que l'institution notifie également sa décision à la préposée cantonale ou au préposé cantonal.

Art. 33

Cet article a été modifié suite à la suppression de la définition d' *« organe »*. Ce terme a ainsi été remplacé par le terme *« institution »* au sens large.

Art. 35 et 36

Par souci de cohérence, ces deux articles sont inversés dans leur ordre d'apparition par rapport à la LIPAD actuelle. Il semble en effet opportun d'énoncer les grands principes de la protection des données, dont la licéité, avant d'entrer dans le détail des exigences de la base légale notamment.

Art. 35

Cette disposition, reprenant les grands principes de la protection des données est calquée sur la nLPD[66], afin de faciliter les futures interprétations par les autorités d'application, et se rapproche se faisant des textes européens[67].

Al. 1

Cet alinéa rappelle l'exigence du principe de licéité, à l'instar de la Convention 108+[68] et de la nLPD[69]. Cela signifie qu'il ne doit pas enfreindre une autre norme du droit suisse visant directement ou indirectement à protéger la personnalité[70].

Al. 2

Cet alinéa rappelle l'exigence du principe de la proportionnalité. Il figure déjà à l'heure actuelle dans la LIPAD[71], mais est remanié pour se rapprocher

[66] Art. 6
[67] FF 2017 6565, p. 6646
[68] Art. 5, par. 3
[69] Art. 6, al. 1
[70] ROSENTHAL, op. cit., ch. 34 et réf. cit.
[71] Art. 36, al. 1 let. a

de la nLPD[72], afin de faciliter les futures interprétations par les autorités d'application.

Elément essentiel du droit de la protection des données, le principe de proportionnalité doit être respecté à toutes les étapes du traitement, y compris au stade initial, c'est-à-dire lorsqu'il est décidé de procéder ou non au traitement des données[73]. Il concerne non seulement les données, mais aussi le choix des moyens et des méthodes de traitement.

Il découle du principe de proportionnalité que seules les données aptes et nécessaires à atteindre les finalités du traitement peuvent être traitées. Par ailleurs, il doit y avoir un rapport raisonnable entre les finalités et le moyen utilisé, les droits de la personne concernée devant être préservés dans la plus large mesure possible (principe de proportionnalité au sens étroit). Les principes d'évitement et de minimisation des données en constituent deux expressions. Le premier implique que si le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée. Le second veut que seules les données absolument nécessaires au but poursuivi soient traitées. Ces deux principes doivent être respectés dès la conception de nouveaux systèmes, et se mêlent ainsi partiellement aux principes de protection des données dès la conception et de protection des données par défaut (voir *infra* commentaire ad art. 37)[74].

L'exigence du respect du principe de proportionnalité figure également dans la Convention 108+[75].

Al. 3

Cet alinéa regroupe les principes de finalité et de reconnaissabilité.

La référence à des *« finalités déterminées »*, à l'instar de la nLPD[76], indique qu'il n'est pas permis de traiter des données pour des finalités non définies, imprécises ou vagues. La légitimité d'une finalité dépendra des circonstances, le but étant de garantir dans chaque cas un juste équilibre entre les droits, les libertés et les intérêts en jeu: le droit à la protection des données à caractère personnel, d'une part, et la protection d'autres droits, d'autre part.

[72] Art. 6, al. 2
[73] Rapport explicatif de la Convention 108+, ch. 40 ad art. 5
[74] FF 2017 6565, p. 6644
[75] Art. 5, par. 1 et par. 4, let. c
[76] Art. 6, al. 3 ; voir aussi art. 5, par. 2, let. b de la Convention 108+ ainsi que l'art. 4, par. 1, let. b de la directive (UE) 2016/679 et l'art. 5, par. 2, let. b RGPD

Un juste équilibre doit ainsi être ménagé entre les intérêts de la personne concernée et ceux du responsable du traitement ou de la société[77].

Par ailleurs, le but et les méthodes du traitement, ainsi que les catégories de données traitées, doivent être globalement reconnaissables pour les personnes concernées selon les règles de la bonne foi.

Cet alinéa mentionne également que les données doivent être traitées ultérieurement de manière compatible avec les finalités initiales. Cette formulation permet de se rapprocher, à l'instar de la nLPD, de la terminologie de la Convention 108+[78]. La notion d'utilisation *« compatible »* implique que les données à caractère personnel ne doivent pas faire l'objet d'un traitement ultérieur que la personne concernée pourrait considérer comme inattendu, inapproprié ou contestable[79]. Un autre exemple classique de traitement des données généralement compatible avec la finalité initiale est la pseudonymisation ou l'anonymisation des données afin de les utiliser à d'autres fins (p. ex. pour les communiquer à un tiers pour lequel elles ne sont plus des données personnelles)[80].

Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier des attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; de la nature des données à caractère personnel ; des conséquences pour les personnes concernées du traitement ultérieur prévu; et de l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu[81].

Al. 4

Selon l'alinéa 4, les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement. Cette

[77] Rapport explicatif de la Convention 108+, ch. 48 ad art. 5
[78] Art. 5, par. 4, let. b
[79] Rapport explicatif de la Convention 108+, ch. 49 ad art. 5
[80] ROSENTHAL, op. cit., ch. 36
[81] Rapport explicatif de la Convention 108+, ch. 49 ad art. 5

exigence correspond à ce que prévoit la nLPD[82] et la Convention 108+[83]. Elle découle aujourd'hui implicitement du principe général de proportionnalité. Le Conseil d'Etat estime toutefois important, à l'instar du Conseil fédéral, compte tenu des évolutions technologiques et des capacités presque illimitées de stockage, de la mentionner expressément. Le respect de ce principe implique que le responsable du traitement fixe des délais de conservation. La deuxième phrase est reprise de l'article 40 LIPAD actuel.

Al. 5

Cet alinéa reprend le principe de l'exactitude des données, à l'instar de la nLPD[84] et des textes européens[85]. Ce principe est déjà prévu dans la LIPAD actuelle mais est remanié pour se rapprocher de la nLPD, afin de faciliter les futures interprétations par les autorités d'application. Le texte prévoit que celui qui traite des données personnelles doit s'assurer qu'elles sont exactes. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Les données qui ne peuvent être rectifiées ou complétées doivent être effacées ou détruites. Le caractère approprié de la mesure dépend notamment du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées. Le devoir d'exactitude peut impliquer selon les cas de tenir les données à jour[86].

Al. 6

Cet alinéa reprend la teneur actuelle de l'article 36, alinéa 2 LIPAD.

Art. 36

Al. 1

[82] Art. 6, al. 4

[83] Art. 5, par. 4, let. e ; voir également l'art. 4, par. 1, let. 3 de la directive (UE) 2016/680 et l'art. 5, par. 1, let. e RGPD

[84] Art. 6, al. 4

[85] Art. 5, par. 3 let. d de la Convention 108+ ; voir également art. 4, par. 1, let. d de la directive (UE) 2016/680 et art. 5, par. 1, let. d RGPD

[86] FF 2017 6565, p. 6646

Cet alinéa reprend, en la modifiant un peu, la teneur de l'article 35, alinéa 1 LIPAD actuel. Il prévoit désormais que les institutions ne peuvent traiter des données personnelles que si une base légale le prévoit ou si l'accomplissement de leurs tâches légales le rend nécessaire.

Al. 2

Cet alinéa concerne plus spécifiquement les traitements de données personnelles sensibles, les activités de profilage et les traitements de données personnelles dont les finalités ou les modalités de traitement sont susceptibles de porter gravement atteinte aux droits fondamentaux de la personne concernée. Un traitement de donnée personnelles non sensibles est susceptible de porter atteinte aux droits fondamentaux d'une personne en fonction des circonstances. Ainsi, le traitement des noms de famille, qui, dans bien des cas ne présente aucun risque pour les individus (par exemple pour l'établissement courant de bulletins de salaire), pourrait impliquer des données sensibles, par exemple s'il a pour finalité de révéler l'origine ethnique ou les convictions religieuses de personnes à partir de l'origine linguistique de leur nom[87].

Cet alinéa prévoit que de tels traitements ne peuvent avoir lieu que si une loi au sens formel le prévoit expressément (base légale directe), ou s'il est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel (base légale indirecte).

Al. 3

Cet alinéa réserve l'application de l'article 36A, qui introduit le consentement de la personne concernée comme élément fondant la licéité du traitement aux conditions restrictives prévues à l'article 36A.

Al. 4

La première phrase de cet alinéa est reprise de l'article 35, alinéa 4 LIPAD actuel. Le législateur l'a depuis mis en œuvre par l'adoption de la loi instituant les numéros d'identification personnels communs, du 20 septembre 2012 (LNIP ; A 2 09).

La 2ème phrase de cet alinéa est nouvelle. Elle abroge la 2ème phrase actuelle de cet alinéa devenue obsolète au vu du changement législatif intervenu au niveau fédéral relatif à l'usage et à la communication du numéro

[87] Rapport explicatif de la Convention 108+, ch. 60 ad art. 6

AVS. En effet, une modification de la loi fédérale sur l'assurance-vieillesse et survivants, du 20 décembre 1946 (LAVS), portant sur l'introduction d'une Quatrième partie spécifique intitulée « *Utilisation systématique du numéro AVS en dehors de l'AVS* » (art. 153b à 153i nLAVS), est entrée en vigueur au 1er janvier 2022. Le but de cette modification est d'accroître l'efficacité des processus administratifs en permettant aux autorités fédérales, cantonales et communales d'utiliser de manière systématique le NAVS pour accomplir leurs tâches légales et faire avancer la cyberadministration[88].

En résumé, les unités des administrations cantonales et communales sont désormais habilitées à utiliser le numéro AVS de manière systématique dans la mesure où l'exécution de leurs tâches légales le requiert (art. 153c nLAVS) et moyennant l'adoption de mesures techniques et organisationnelles destinées à protéger les données (art. 153d nLAVS); la communication du numéro AVS dans l'application du droit cantonal ou communal étant pour le surplus régie par l'article 153g nLAVS.

Art. 36A

Al. 1

Cet alinéa introduit un fait justificatif extra-légal dérogeant aux exigences de l'article 36. Il vise à autoriser les institutions à traiter des données également dans le cas où la personne concernée a donné son consentement Une disposition similaire est prévue dans la nLPD[89]. Cette formulation permet par ailleurs, à l'instar de la nLPD, de se rapprocher de la terminologie de la Convention 108+[90], afin de satisfaire aux exigences de celui-ci.

Al. 2

Pour être considéré comme valable, le consentement doit avoir été exprimé librement et après que la personne concernée ait été dûment informée, et doit porter sur un ou plusieurs traitements déterminés. Il doit être exprès en cas de traitement de données personnelles sensibles ou de profilage.

Pour que le consentement soit valable, il faut toujours que le traitement, en particulier son ampleur et son but, soit suffisamment défini. Le

[88] Voir message du 18 décembre 2020 "Utilisation systématique du numéro AVS par les autorités", RO 2021 758; FF 2019 6955
[89] Art. 34, al. 4, let. b
[90] art. 5, par. 2 ; voir également art. 6 par. 1 let. a RGPD

consentement peut porter sur plusieurs traitements identiques ou différents. Il est également possible que le but du traitement nécessite plusieurs traitements. Le consentement doit couvrir le but du traitement auquel il sert de motif justificatif. Si les données sont traitées à d'autres fins que celles qui ont fait l'objet d'un consentement, ce traitement doit être justifié par d'autres motifs[91].

Le consentement doit en outre être clair. Il faut donc que la déclaration de la personne concernée exprime la volonté de celle-ci sans ambiguïté. Tout dépend des circonstances concrètes de chaque cas particulier. Conformément au principe de la proportionnalité, on considère que plus les données sont sensibles, plus le consentement doit être clair[92].

Le présent projet, à l'instar de la nLPD, ne prévoit pas de forme particulière pour le consentement. En particulier, il n'est pas lié à une déclaration écrite. La personne concernée peut donner un consentement clair au sens de l'alinéa 2 par la manifestation tacite de sa volonté. Tel est le cas lorsque la manifestation de la volonté ne découle pas de la déclaration elle-même, mais d'un comportement qui, compte tenu des circonstances dans lesquelles il se produit, peut être compris comme l'expression claire de la volonté. Mais la manifestation de la volonté est nécessaire; le simple silence ou l'inaction ne peuvent constituer un consentement valable[93]. Pour les mêmes raisons, des formulaires ou cases à cocher prévalidés ne peuvent constituer un consentement.

Selon la seconde phrase de l'alinéa 2, le consentement doit être exprès lorsque le traitement concerne des données sensibles ou consiste en un profilage. Un consentement exprès est l'accord d'une personne exprimé d'une manière apparente, telle qu'une signature ou une déclaration verbale non équivoque. Une déclaration de volonté est *« expresse »* lorsqu'elle est formulée oralement, par écrit ou par un signe, et découle directement des mots ou du signe employé. La déclaration de volonté en tant que telle doit manifester clairement la volonté dans sa forme même. Cela peut se faire notamment en signant un document ou en cochant une case. Lorsqu'un consentement exprès est requis, il ne peut pas être tacite[94].

[91] FF 2017 6565, p. 6647
[92] FF 2017 6565, p. 6647
[93] FF 2017 6565, p. 6647
[94] Antoine Amiguet, Phillippe Fischer, Changement de paradigme en matière de protection des données, in Revue de l'avocat 2018, pp. 18ss

Al. 3

Cet alinéa prévoit que le consentement peut être révoqué en tout temps et sans motifs. En effet, aucune influence ou pression indues (de nature économique ou autre), directe ou indirecte, ne peut être exercée sur la personne concernée et son consentement ne doit pas être considéré comme libre si elle n'a pas de véritable choix ou de liberté de choix, ou ne peut refuser ou retirer son consentement sans subir de préjudice[95]. La seule réserve est celle du délai raisonnable qui pourrait être nécessité pour des raisons techniques.

Al. 4

Cet alinéa correspond à l'article 10, lettre b, de la directive (UE) 2016/680 et à l'article 6, paragraphe 1, lettre d, du RGPD[96]. En vertu de cette disposition, les institutions peuvent traiter des données personnelles si le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, y compris leur intégrité physique ou leur vie[97]. Il vise également les cas où le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine (conflit armé ou autre type de violence)[98].

Al. 5

Cet alinéa introduit un 2ème fait justificatif extra-légal dérogeant aux exigences de l'art. 36. Il vise à autoriser les institutions à traiter des données également dans les cas où la personne concernée a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée

[9595] Rapport explicatif de la Convention 108+, ch. 42 ad art. 5 ; voir également consid. 42 du RGPD

[96] Voir également Rapport explicatif de la Convention 108+, ch. 46 et 47 ad art. 5

[97] Voir consid. 112 du RGPD

[98] Voir Rapport explicatif de la Convention 108+, ch. 47 ad art. 5 ; voir également consid. 46b du RGPD

expressément au traitement. Une disposition similaire est aussi prévue dans la nLPD[99].

Art. 36B

Cette disposition s'inspire de l'article 33 nLPD, qui met en œuvre l'article 21 de la directive (UE) 2016/680**[100]**, afin de faciliter les futures interprétations par les autorités d'application.

Elle prévoit que lorsque deux institutions ou plus déterminent conjointement les finalités et les moyens du traitement elles sont responsables conjointes du traitement et doivent définir de manière transparente leurs obligations respectives dans la déclaration au registre des activités de traitements, soit CATTRAIT selon sa nouvelle appellation du fait de la disparition de la notion de *« fichier »* (à ce sujet, voir *infra* commentaire ad art. 43).

Art. 36C

Cet article reprend, pour l'essentiel, la teneur de l'article 13A RIPAD. Il précise de plus, à l'alinéa 1, lettre a que seuls les traitements que le responsable du traitement est en droit de réaliser peuvent être sous-traités (voir *infra*).

Al. 1 et 2

Cet alinéa pose le cadre légal général de la sous-traitance. Il est calqué sur l'article 9 nLPD, afin de faciliter les futures interprétations par les autorités d'application.

Le contrat liant le responsable du traitement et le sous-traitant peut être de nature diverse. Il peut s'agir d'un mandat (art. 394ss CO[101]), d'un contrat d'entreprise (art. 363ss CO) voire d'un contrat mixte selon les obligations du sous-traitant. Le sous-traitant cesse d'être un tiers à compter du moment où il débute ses activités contractuelles pour le compte du responsable du traitement[102].

[99] Art. 34, al. 4, let. b.
[100] Voir également art. 26 RGPD
[101] Loi fédérale complétant le Code civil suisse (Livre cinquième: Droit des obligations), du 30 mars 1911 ; RS 220
[102] FF 2017 6565, p. 6643

Ces alinéas instituent un devoir de diligence à la charge du responsable du traitement, dans le but de sauvegarder les droits des personnes concernées en cas de sous-traitance. Le responsable du traitement doit s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui[103]. Cela concerne principalement le respect des principes généraux de protection des données, les règles relatives à la sécurité, ainsi que le respect des droits des personnes concernées (art. 44ss LIPAD). Le contrat de sous-traitance ne doit en effet pas faire obstacle à l'obligation de l'institution de respecter en tout temps ses obligations aux termes des articles 44ss LIPAD relatifs aux droits des personnes concernées (notamment droit d'accès à ses données personnelles, droit de demander la rectification, la destruction ou encore d'en constater le caractère illicite, voire d'exiger la fin du traitement illicite). Le responsable du traitement doit, par analogie avec l'article 55 CO, mettre tout en œuvre pour éviter d'éventuelles violations de la LIPAD. Il doit ainsi veiller à choisir soigneusement son mandataire, à lui donner les instructions adéquates et à exercer la surveillance nécessaire[104]. La Convention 108+ prévoit elle aussi une obligation similaire[105].

L'obligation de prévoir la possibilité de faire des audits chez le sous-traitant précise et renforce les mesures de sécurité qui doivent être mises en place, et permet de s'assurer de leur efficacité.

Al. 3

Cet alinéa exige que l'institution donne expressément son accord à une sous-traitance en cascade et que le contrat conclu oblige le sous-traitant du premier niveau à veiller au respect des mêmes prescriptions de protection dans la suite de la chaîne de sous-traitance. L'accord préalable écrit est également une exigence de la directive (UE) 2016/680[106].

Al. 4

Cet alinéa prévoit explicitement que l'institution demeure responsable des données personnelles qu'elle fait traiter par des tiers. Cette responsabilité s'étend naturellement également aux données personnelles dont le traitement aurait été délégué par le sous-traitant à un autre sous-traitant (sous-traitance en cascade).

[103] FF 2017 6565, p. 6651
[104] FF 2017 6565, p. 6651
[105] Art. 10 par. 1h
[106] Art. 22 par. 2

Al. 5

Cet alinéa fusionne la problématique de la sous-traitance et celle de la communication transfrontière de données, y compris le recours à des systèmes d'information délocalisés ou dématérialisés, ceux-ci n'étant finalement qu'un cas de sous-traitance à l'étranger.

La notion de *« niveau de protection adéquat »* a été choisie afin de suivre celle choisie au niveau fédéral[107], au niveau européen[108] ainsi que dans la Convention 108+[109]. Elle ne se recoupe pas entièrement avec celle de *« niveau de protection équivalent »* utilisée à l'article 39 LIPAD, cette dernière pouvant être plus restrictive. A noter toutefois que les deux notions pourraient être amenées à se recouper largement.

Il est rappelé en outre que le terme *« traitement »* recouvre tant des traitements complets que partiels de données personnelles.

Il convient encore de préciser qu'il a été renoncé ici à réglementer spécifiquement l'usage des réseaux sociaux par le Petit et le Grand Etat (Facebook, Twitter, etc.) dans la mesure où les citoyens y recourant le font sur une base volontaire, le plus souvent en entrant dans un rapport de droit direct avec le gestionnaire de la plate-forme privée et après avoir eux-mêmes créé un compte et accepté les conditions générales de ces instruments – dont la récolte des données personnelles (adresse IP et autres informations laissées sur leurs comptes publics). Dès lors, ces situations peuvent être appréhendées par les règles générales relatives au consentement des personnes concernées.

Art. 37

Cet article instaure l'obligation de protéger les données dès la conception (*« privacy by design »*) et par défaut (*« privacy by default »*), le second concept étant inclus dans le premier.

Il est calqué sur l'article 7 nLPD, afin de faciliter les futures interprétations par les autorités d'application, et met en œuvre, à l'instar de ce

[107] Art. 16 nLPD
[108] Art. 36 directive (UE) 2016/680 ; art. 45 RGPD
[109] Voir article 14 (le terme adéquat est ici remplacé par approprié ; voir toutefois Rapport explicatif de la Convention 108+, ch. 112 ad art. 14)

dernier, les exigences de la Convention 108+[110] et de la directive (UE) 2016/680[111]. Le RGPD contient une règle similaire[112].

Al. 1

Cet alinéa traite de la protection des données dès la conception (*« privacy by design »*). Cette dernière se caractérise par des mesures proactives visant à prévenir et minimiser les risques d'atteintes aux droits des personnes concernées. L'obligation débute ainsi en amont des opérations de traitement, avant la collecte des données. Son but est d'assurer un traitement conforme à la loi du début à la fin du traitement des données (i. e. de la collecte à la suppression de la donnée, y compris l'archivage). Ce principe ne doit pas être confondu avec la protection des données par défaut (*« privacy by default »*), qui exige de traiter le moins de données possibles par des préréglages appropriés (voir *infra* commentaire ad alinéa 3). Les deux principes n'en restent pas moins étroitement liés, dans la mesure où de telles fonctionnalités doivent être intégrées dès la conception[113].

La protection technique des données personnelles ne s'appuie pas sur une technologie précise; elle passe plutôt par la mise en place de règles techniques et organisationnelles conformes aux principes définis aux articles 35 et 37A du présent projet. En d'autres termes, les exigences légales auxquelles doit satisfaire un traitement conforme à la protection des données sont déjà intégrées dans le système, de manière à rendre impossible une violation de la protection des données ou d'en réduire la probabilité.

Il s'agit par exemple de la fixation d'échéances régulières pour l'effacement ou l'anonymisation systématique des données personnelles. Un principe significatif pour la protection des données au plan technique est celui de la *minimisation des données*, qui ressort aussi de l'article 35 du présent projet. Selon ce dernier, il faut fixer avant même le début d'un traitement ses modalités, de manière à ce que le moins de données possible

[110] Art. 10 par. 3 et Rapport explicatif de la Convention 108+, ch. 89 ad art. 10

[111] Art. 20

[112] Art. 25

[113] LECHTMAN, L'obligation de *« privacy by design »* en Suisse et son implémentation dans les études d'avocat, in Anwalts 10/2020, p. 403ss et réf. cit.

soient traitées, et de façon à ce qu'elles soient conservées le moins longtemps possible[114].

Al. 3

Cet alinéa traite du principe de la protection des données par défaut.

Le responsable du traitement est tenu, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie (*principe de la minimisation des données*), pour autant que la personne concernée n'en dispose pas autrement (*« privacy by default »*)[115]. Les systèmes d'information et les applications traitant des données personnelles doivent ainsi être paramétrés, par défaut, de la manière la plus favorable à la protection de la vie privée.

Le lien avec la protection des données dès la conception est étroit. En effet, ces réglages prédéfinis s'inscrivent souvent dans un système entier respectueux de la protection des données. Ce qui est spécifique à la protection des données par défaut, c'est l'influence éventuelle de la personne concernée. Alors qu'elle ne peut en principe pas modifier le système lui-même, elle a toujours la possibilité, s'agissant des réglages par défaut, de choisir une solution différente (article 37, alinéa 3 du présent projet). La protection des données par défaut permet en conséquence à la personne concernée de consentir à un traitement déterminé[116].

Art. 37A

Cet article est globalement calqué sur l'article 8 nLPD, afin de faciliter les futures interprétations par les autorités d'application.

Al. 1

Le devoir d'assurer la sécurité des données est une exigence de la Convention 108+[117] et de la directive (UE) 2016/680[118]. Le RGPD prévoit

[114] FF 2017 6565, p. 6648-6649

[115] FF 2017 6565, p. 6649; voir également Rapport explicatif de la Convention 108+, ch. 89 Ad art. 10

[116] FF 2017 6565, p. 6649-6650; voir également Rapport explicatif de la Convention 108+, ch. 89 ad art. 10

[117] Art. 7

[118] Ar. 4 §1, let. f Directive (UE) 2016/690

une règle comparable[119]. Les institutions au sens de l'article 3 LIPAD doivent ainsi assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Ces mesures doivent permettre d'éviter toute violation de la sécurité des données personnelles.

Cette disposition matérialise l'approche fondée sur les risques. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées[120].

Al. 2

L'alinéa 2 mentionne le but des mesures. Ces dernières doivent permettre d'éviter toute violation de la sécurité des données, soit toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite (art. 4 let. j du présent projet). Les mesures peuvent viser par exemple à pseudonymiser des données, à assurer la confidentialité et la disponibilité du système ou de ses services, ou encore à élaborer des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures prises[121].

Il existe une interaction entre la protection des données et leur sécurité, mais ces deux aspects doivent être traités séparément. La protection des données relève de la protection de la personnalité de l'individu. Quant à la sécurité des données, elle vise généralement les données présentes chez un responsable du traitement ou chez un sous-traitant et englobe le cadre organisationnel et technique général du traitement des données. Par conséquent, la protection de l'individu n'est possible que si des mesures techniques générales ont été prises pour la sécurité des données le concernant. D'où la distinction opérée entre l'obligation d'assurer la sécurité des données au sens du présent article et la protection des données dès la conception visée à l'article 37 du présent projet. L'article 37A du présent projet oblige les institutions à prévoir, pour leurs systèmes, une architecture de sécurité appropriée et à les protéger contre les maliciels ou la perte de données, par exemple. L'article 37 du présent projet vise, par contre, à garantir, par des moyens techniques, le respect de prescriptions de protection

[119] Art. 5 §1, let. f et 32 RGPD
[120] FF 2017 6565, p. 6650
[121] FF 2017 6565, p. 6650

de données, par exemple la proportionnalité du traitement des données. Certaines mesures, comme l'anonymisation des données, peuvent à cet égard se révéler significatives pour les deux obligations[122].

Al. 3

Conformément à cet alinéa, les exigences minimales en matière de sécurité des données personnelles seront déterminées par le Conseil d'Etat par voie règlementaire.

Al. 4

Cet alinéa prévoit, conformément à la directive (UE) 2016/680[123] que les institutions sont tenues de contrôler périodiquement le respect des mesures de sécurité mises en place. Le projet d'Ordonnance relative à la loi fédérale sur la protection des données (OLPD) mis en consultation par le Département fédéral de justice et police (DFJP) prévoit également cette obligation[124].

Art. 37B

Cet article prévoit l'obligation de procéder à une analyse d'impact relative à la protection des données personnelles. Il s'inspire de l'article 22 nLPD, afin de faciliter les futures interprétations par les autorités d'application et concrétise, à l'instar de ce dernier, les exigences posées par la Convention 108+[125] et la directive (UE) 2016/680[126]. Le RGPD contient des dispositions similaires[127].

L'analyse d'impact est un instrument destiné à identifier et à évaluer les risques que certains traitements de données personnelles pourraient entraîner pour la personne concernée. Le cas échéant, cette analyse doit servir à définir des mesures pour faire face à ces risques. L'avantage pour le responsable du traitement est qu'elle permet d'anticiper d'éventuels problèmes juridiques liés à la protection des données et d'éviter les coûts qui pourraient en résulter[128].

[122] FF 2017 6565, p. 6650
[123] Art. 19 par. 1 ; le RGPD prévoit une règle similaire à l'art. 24 par. 1
[124] Art. 1, al. 2 P-OLPD.
[125] Art. 10 par. 2
[126] Art. 27
[127] Art. 35ss
[128] FF 2017 6565, p. 6676

Al. 1

L'analyse d'impact doit être menée par le responsable du traitement avant la mise en œuvre du traitement. Le responsable du traitement doit procéder à une telle analyse lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Le risque doit être analysé au cas par cas en termes de gravité et de vraisemblance.

Le responsable du traitement est donc tenu de faire un pronostic des conséquences que le traitement en question peut avoir pour la personne concernée[129].

Al. 2

L'alinéa 2 précise que l'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Plus le traitement est étendu, plus les données sont sensibles et plus la finalité du traitement est vaste, plus il y a lieu de conclure à un risque élevé. L'alinéa 2 mentionne trois exemples dans lesquels un tel risque existe:

- selon la lettre a, c'est le cas lorsque le traitement concerne un grand volume de données sensibles, comme cela peut se produire dans le cadre de projets de recherche médicaux ;
- la lettre b dispose qu'un risque élevé existe en cas de profilage ; tel peut être également le cas lorsque des décisions sont prises exclusivement sur la base d'un traitement de données personnelles automatisé, y compris en cas de profilage, et que ces décisions ont des effets juridiques sur la personne concernée ou l'affectent de manière notable[130] ;
- selon la lettre c, enfin, il y a un risque élevé lorsqu'il s'agit de la surveillance de grandes parties du domaine public (par ex: la surveillance d'un hall de gare)[131].

Al. 3

Selon l'alinéa 3, l'analyse d'impact relative à la protection des données contient notamment une description du traitement envisagé. Il faut ainsi

[129] FF 2017 6565, p. 6676
[130] FF 2017 6565, p. 6677
[131] FF 2017 6565, p. 6677

présenter les différents processus (par ex. la technologie employée), la finalité du traitement ou la durée de conservation des données personnelles. Par ailleurs, l'analyse d'impact doit montrer quels risques le traitement implique pour la personnalité ou les droits fondamentaux de la personne concernée. Il s'agit ici d'un approfondissement de l'évaluation des risques qui doit déjà être faite en amont, lors de l'examen de la nécessité de procéder à une analyse d'impact. Il convient ainsi de présenter la nature du risque élevé qu'engendre le traitement envisagé et les moyens de l'évaluer. Enfin, l'analyse d'impact doit expliquer les mesures prévues pour faire face à ce risque. Il s'agira souvent de mettre en œuvre les principes de l'article 35 du présent projet, ainsi que les principes de protection dès la conception et par défaut (*« privacy by design/by default »*; article 37 du présent projet). A cette occasion, il est possible de mettre en balance les intérêts de la personne concernée et ceux du responsable du traitement. Cette confrontation des intérêts doit être dûment motivée et intégrée dans l'analyse d'impact. [132].

La réalisation de l'analyse d'impact doit être menée sans formalités excessives dans le respect du principe de proportionnalité[133].

Al. 4

Conformément à l'article 56, alinéa 3, lettre e LIPAD, la préposée cantonale ou le préposé cantonal exprime son avis sur les projets d'actes législatifs ayant un impact en matière de protection des données personnelles. Le présent alinéa prévoit ainsi que lorsque l'analyse d'impact est requise au sens de l'alinéa 1 du présent article, elle doit être jointe au projet d'acte législatif soumis à la préposée cantonale ou au préposé cantonal.

Bien qu'elle ne soit pas prescrite par la Convention 108+, cette consultation préalable correspond à la réglementation européenne[134]. Elle est reprise dans le présent projet pour permettre à la préposée cantonale ou au préposé cantonal d'exercer une fonction de conseil et de prévention, sans compter qu'elle offre une plus grande efficacité aux responsables du traitement en ce sens que les difficultés qui pourraient surgir en lien avec le traitement sont déjà éliminées à un stade précoce[135].

[132] FF 2017 6565, p. 6678
[133] Rapport explicatif de la Convention 108+, ch. 88 ad art. 10
[134] Art. 28 de la directive [UE] 2016/680 et art. 36 RGPD
[135] FF 2017 6565, p. 6678

Cela permet également au législateur d'évaluer les risques éventuels pour la personne concernée au regard du but du traitement et d'édicter, le cas échéant, des prescriptions pour y faire face[136].

Art. 37C

Le présent article s'inspire de l'article 24 nLPD, afin de faciliter les futures interprétations par les autorités d'application. Il instaure l'obligation d'annoncer toute violation de la sécurité des données personnelles[137].

Cette disposition concrétise les exigences fixées par la Convention 108+[138] et la directive (UE) 2016/680[139]. Le RGPD contient des dispositions similaires[140].

Les mesures à prendre en cas d'incident entrainant une violation de la sécurité des données au sens de l'article 4, lettre j du présent projet portent sur trois niveaux :

a) identification de la violation et correction (alinéa 1) ;

b) consignation, dans un document interne, de la nature de la violation, du type de données concernées et des catégories de personnes touchées, des conséquences probables pour ces dernières et des mesures prises pour y remédier (alinéa 2) ; et

c) annonce de la violation lorsque cela est nécessaire à la préposée cantonale ou au préposé cantonal ou aux personnes concernées (alinéas 3 et 4, sous réserve de l'alinéa 5).

Al. 1

Cet alinéa prévoit que le responsable du traitement doit prendre immédiatement les mesures appropriées, lorsqu'il constate une violation de la sécurité des données, afin de mettre fin à la violation et d'en minimiser les effets et en informe immédiatement sa conseillère ou son conseiller à la protection des données et à la transparence.

Al. 2

[136] FF 2017 6565, p. 6678
[137] Cette notion est définie à l'art. 4 let. j du présent projet
[138] Art. 7 par. 2
[139] Art. 30-31
[140] Art. 33-34

Le responsable du traitement doit documenter, dans un document interne, la nature de la violation, le type de données concernées et les catégories de personnes touchées, les conséquences probables pour ces dernières et les mesures prises pour y remédier. Le projet d'OLPD mis en consultation prévoit une obligation similaire à son article 19, alinéa 5.

Al. 3

Le présent projet n'exige pas, à l'instar de l'article 24 nLPD, que tout incident doive être annoncé à la préposée cantonale ou au préposé cantonal. Seuls sont visés les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

Al. 4

Cet alinéa prévoit que le responsable du traitement doit informer la personne concernée lorsque cela est nécessaire à sa protection ou lorsque la préposée cantonale ou le préposé cantonal l'exige.

Il existe une marge d'appréciation assez large pour déterminer si la première condition est réalisée. Il faut se demander notamment si l'information peut réduire les risques pour la personnalité ou les droits fondamentaux de la personne concernée, en lui permettant notamment de prendre les dispositions nécessaires pour se protéger (modification des données d'accès ou du mot de passe, par ex.)[141].

Al. 5

Cet alinéa prévoit les conditions auxquelles le responsable du traitement peut restreindre l'information de la personne concernée, la différer ou y renoncer.

Le devoir d'informer est réputé impossible à respecter lorsque le responsable du traitement n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données. On estime de même que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées. C'est notamment dans ces cas de figure que peut s'appliquer la lettre f: cette disposition autorise le responsable du

[141] FF 2017 6565, p. 6682

traitement à opter pour une communication publique si l'information des personnes concernées est garantie de manière équivalente. On estime que cette condition est remplie quand une annonce individuelle ne permettrait pas d'améliorer sensiblement l'information de la personne concernée[142].

Art. 38

A l'instar de l'article 19 nLPD, cet article traite du devoir du responsable du traitement d'informer la personne concernée lors de la collecte de données personnelles.

Ces exigences se retrouvent dans la Convention 108+[143] ainsi que dans la directive (UE) 2016/680[144]. Le RGPD contient une réglementation similaire.

Le devoir d'informer renforce la transparence des traitements, ce qui est l'un des principaux buts de la révision[145]. Le responsable du traitement est tenu de faire preuve de transparence dans la conduite des opérations de traitement afin de garantir un traitement loyal et de permettre aux personnes concernées de comprendre et, partant, d'exercer pleinement leurs droits dans le cadre du traitement considéré[146]. L'amélioration de la transparence du traitement des données personnelles entraîne donc aussi un renforcement des droits de la personne concernée, autre but important de la révision. Enfin, le devoir d'informer contribue à sensibiliser la population sur la protection des données, qui est aussi un objectif de la révision[147].

Al. 1 et 2

Le présent projet, à l'instar de la nLPD, ne précise pas la forme que doit revêtir l'information. Le responsable du traitement doit veiller à ce que la personne concernée puisse effectivement prendre connaissance de celle-ci par un moyen facilement accessible, mais pas à ce qu'elle s'informe effectivement.

Une information générale peut suffire si les données sont collectées auprès de la personne concernée[148]. Les informations peuvent être fournies

[142] FF 2017 6565, p. 6682
[143] Art. 8
[144] Art. 13
[145] FF 2017 6565, p. 6668
[146] Rapport explicatif de la Convention 108+, ch. 67 ad art. 8
[147] FF 2017 6565, p. 6668
[148] FF 2017 6565, p. 6668

sous tout format approprié (par le biais d'un site web, d'outils technologiques sur des appareils personnels, etc.) dès lors qu'elles sont présentées de manière effective et loyale à la personne concernée[149].

Si les données personnelles ne sont pas collectées auprès de la personne concernée, le responsable du traitement doit réfléchir à un moyen qui permette à celle-ci de prendre effectivement connaissance de l'information. La simple mise à disposition des informations peut ne pas suffire. Il faut informer activement la personne concernée, que ce soit d'une manière générale ou personnalisée. Le devoir d'information vise en effet aussi à éviter que des données concernant une personne soient traitées à l'insu de celle-ci. Les exceptions visées à l'article 38A sont réservées.

L'information n'est soumise à aucune exigence de forme, mais il faut de manière générale en choisir une qui respecte le principe de la transparence des données. Pour des raisons de preuve, il est en outre recommandé de documenter l'information ou d'y procéder par écrit. Par ailleurs, l'information doit être rédigée de manière suffisamment claire pour atteindre son but, à savoir la transparence du traitement des données.

La liste des informations que le responsable du traitement doit fournir à la personne concernée au sens de l'alinéa 2 n'est pas exhaustive ; il s'agit uniquement des informations minimales à fournir dans ce cadre.

Le responsable du traitement est libre de décider s'il préfère indiquer les destinataires ou les catégories de destinataires. Comme dans l'Union européenne[150], les sous-traitants font partie des destinataires au sens de la disposition. Si le responsable du traitement ne souhaite pas révéler l'identité des destinataires, il peut se contenter d'indiquer leur catégorie. Le degré de détails de l'information dépendra du type de données personnelles traitées ainsi que de la nature et de l'ampleur du traitement. Il est ainsi par exemple possible que l'on doive informer sur la durée du traitement ou l'anonymisation de données. Cette souplesse est nécessaire si l'on veut tenir compte de tous les types de traitements possibles. Elle garantit par ailleurs que seules les informations nécessaires sont transmises.[151].

Al. 3

En cas de communication de données personnelles à l'étranger, le responsable du traitement doit communiquer en outre à la personne, en sus

[149] Rapport explicatif de la Convention 108+, ch. 68 ad art. 8
[150] Art. 4 par. 9 RGPD
[151] FF 2017 6565, p. 6668

des informations mentionnées à l'alinéa 2, le nom de la corporation ou de l'établissement de droit public auquel elles sont communiquées et, le cas échéant, l'application d'une des exceptions prévues à l'article 39, alinéa 7. Cet alinéa transpose la solution fédérale au droit genevois existant.

Al. 4

Dans l'hypothèse où les données personnelles ne sont pas collectées auprès de la personne concernée, le responsable du traitement lui communique les informations mentionnées aux alinéas 2 à 3 dans les meilleurs délais, mais au plus tard lors de leur utilisation. Le présent projet laisse ainsi une marge d'appréciation au responsable du traitement en fonction des circonstances, tout en lui imposant de le faire au plus tard lors de l'utilisation effective des données.

Art. 38A

Cet article mentionne les cas dans lesquels le responsable du traitement est délié du devoir d'information au sens de l'article 38 du présent projet.

Al. 1

Cet alinéa s'inspire de la nLPD[152] et de la Convention 108+[153]. Le RGPD contient des règles similaires[154].

Conformément à la lettre b, le responsable du traitement est délié du devoir d'information si le traitement des données est prévu par la loi (tant formelle que matérielle).

L'information est impossible au sens de la lettre c lorsque la personne concernée n'est pas identifiable, par exemple parce qu'il s'agit de la photo d'un inconnu. Cela dit, il ne suffit pas de supposer que l'identification est impossible. Il faut procéder à un minimum de recherches, dans les limites du raisonnable[155].

Les efforts déployés pour informer la personne concernée sont disproportionnés au sens de la lettre c dès lors qu'ils paraissent injustifiés par rapport au bénéfice que la personne concernée retirerait de l'information. Il faut notamment tenir compte du nombre de personnes concernées.

[152] Art. 20
[153] Art. 8 par. 2 et 3
[154] Art. 14 par. 5
[155] FF 2017 6565, p. 6671

L'information nécessite par exemple des efforts disproportionnés lorsque des données sont traitées uniquement à des fins d'archivage d'intérêt public. L'information de toutes les personnes concernées supposerait régulièrement des efforts considérables, tout en présentant un intérêt souvent limité en raison de l'ancienneté des données, par exemple. Cette dernière exception doit être interprétée de manière restrictive: le responsable du traitement ne doit pas se contenter d'une supposition. Il doit déployer tous les efforts qu'on est en droit d'attendre de lui dans le cas d'espèce pour remplir son devoir d'information. Ce n'est que si ses efforts restent vains que l'on considérera que l'information n'est pas possible[156].

Al. 2

Contrairement à l'alinéa 1, cet alinéa englobe les configurations dans lesquelles il y a pesée des intérêts. En fonction de la pesée des intérêts, le responsable du traitement renonce à la communication des informations, la restreint ou la diffère. Cette disposition doit être interprétée restrictivement. L'information ne doit pas être limitée au-delà de ce qui est absolument nécessaire et son motif doit être mis en relation avec l'intérêt à la transparence du traitement. De manière générale, on choisira la solution la plus favorable à la personne concernée, garantissant la transparence maximale du traitement compte tenu des circonstances[157].

Cette disposition vise par exemple les cas dans lesquels les informations concernant le traitement des données personnelles de la personne concernée contiennent aussi des informations sur des tiers. Dans certains cas, les intérêts de ce tiers peuvent être lésés par l'accomplissement du devoir d'information[158].

La nLPD mentionne, à titre d'intérêt public prépondérant, la sûreté intérieure ou extérieure de la Suisse ou le cas où la communication des informations est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative[159].

Art. 38B

[156] FF 2017 6565, p. 6671
[157] FF 2017 6565, p. 6672
[158] FF 2017 6565, p. 6672
[159] Voir également dans ce cadre l'art. 13, par. 3 de la directive (UE) 2016/680 et art. 23 RGPD

A l'instar de l'article 21 nLPD, de la Convention 108+[160] et de la directive (UE) 2016/680[161], cet article règlemente le devoir d'informer la personne concernée en cas de décision individuelle automatisée. Le RGPD[162] prévoit des règles similaires.

L'introduction de la notion de décision individuelle automatisée est nécessaire car ces décisions sont de plus en plus fréquentes en raison du développement technologique. Une décision individuelle automatisée implique en tout cas qu'il n'y ait eu aucune décision prise par une personne physique sur la base de sa propre évaluation de la situation. Ainsi, il y a décision individuelle automatisée lorsqu'une exploitation de données a lieu sans intervention humaine et qu'il en résulte une décision, ou un jugement, à l'égard de la personne concernée[163].

L'expression *« décisions individuelles automatisées »* ne désigne ainsi que les décisions pour lesquelles une machine dispose d'un pouvoir d'appréciation. La machine prend une décision sur la base d'une évaluation des données personnelles à sa disposition, que la machine les ait *« apprises »* ou qu'un être humain les ait programmées. Ainsi, seules les décisions qui sont entièrement prises par une machine et qui supposent un pouvoir d'appréciation sont concernées, c'est-à-dire celles qui requièrent une évaluation ou une interprétation. Le système de contrôle d'accès, qui déverrouille la porte lorsqu'un badge valable est présenté, ne prend aucune décision individuelle automatisée car il n'y a pas de place pour l'interprétation. En outre, aucune décision individuelle automatisée n'est prise s'il existe un accord préalable avec la banque selon lequel le compte bénéficie d'une autorisation de découvert jusqu'à CHF 1000 et si le distributeur automatique de billets applique strictement cette limite. Le distributeur automatique de billets ne prend pas de décision, il en applique simplement une. Si, en revanche, la banque laisse son ordinateur déterminer une limite de découvert individuelle pour chaque client – sur la base de ses entrées et sorties de paiements – il s'agit d'une décision individuelle automatisée. Il n'y a pas de décision individuelle automatisée lorsqu'un ordinateur suggère des limites de découvert individuelles à un employé de banque, mais que celles-ci sont finalement approuvées par l'employé. Du point de vue de la protection des données, il s'agit d'un profilage (l'ordinateur évalue la solvabilité du client concerné de manière entièrement

[160] Art. 9 let. a
[161] Art. 11
[162] Art. 22
[163] FF 2017 6565, p. 6674

automatique), mais aucune décision n'est prise de manière automatisée. Dans ce contexte, le fait qu'une décision prise par une machine soit communiquée par la machine ou par un être humain (et que l'être humain ne puisse ou ne doive plus influencer la décision) est sans importance[164].

Dans le domaine public on peut penser à l'émission d'une décision de taxation, l'envoi d'une amende pour excès de vitesse, ou encore au versement de prestations d'assurance.

Il n'est pas nécessaire que la personne concernée soit informée de chaque décision individuelle automatisée, mais seulement lorsque la décision a pour elle des effets juridiques ou l'affecte de manière significative. De tels effets sont admis, par exemple, en cas de taxation fiscale automatique. On peut supposer que la personne concernée est affectée de manière significative lorsqu'elle est durablement entravée sur le plan économique ou personnel. Une simple nuisance ne suffit pas[165].

Al. 2

A la base des décisions individuelles automatisées se trouvent des algorithmes. A la demande de la personne ayant fait l'objet d'une telle décision, le responsable du traitement lui communique la logique et les critères à la base de celle-ci. Cette garantie est nécessaire pour permettre à la personne concernée d'apprécier le bien-fondé de la décision avant d'éventuellement la contester. Elle est prévue par l'article 9, chiffre 1, lettre d de la Convention 108+, qui stipule que toute personne a le droit d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués. Cette demande ne suspend toutefois pas le délai prévu à l'alinéa 3.

Al. 3

Cet alinéa introduit la possibilité, pour toute personne ayant fait l'objet d'une décision individuelle automatisée, de former une réclamation, dans les 30 jours à compter de sa notification, auprès de la même autorité.

Al. 4

Cet alinéa précise que la décision sur réclamation ne peut pas être rendue de manière automatisée, afin de garantir qu'une personne physique se penche sur la réclamation.

---

[164] Rosenthal, op. cit., ch. 108
[165] FF 2017 6565, p. 6674

Al. 5

Cet alinéa réserve les procédures de réclamation prévue par des lois spéciales.

Art. 39

Cet article a été modifié suite à la suppression de la définition d'« *organe* ». Ce terme a ainsi été remplacé par le terme *« institution »*. De même, suite au changement de terminologie, le terme *« responsable »* (au sens de l'article 50 LIPAD) a été remplacé par les termes *« conseillère ou conseiller à la protection des données et à la transparence »* (voir également *infra* commentaire ad art. 50).

Par ailleurs, l'alinéa 11 a été complété afin de prévoir que l'institution requise communique sa décision non seulement aux parties et aux personnes consultées, mais également à la préposée cantonale ou au préposé cantonal.

Art. 41

Cette disposition est calquée sur l'article 39 nLPD, afin de faciliter les futures interprétations par les autorités d'application.

Cette disposition vise deux situations: premièrement, celle où une entité traite les données qu'elle détient à des fins ne se rapportant pas à des personnes; deuxièmement, celle où elle communique les données à des organes de la Confédération ou des cantons, ou encore à des personnes privées, à des fins de recherche, de planification ou de statistique[166].

Le 1er alinéa énonce à quelles conditions une entité soumise à la LIPAD peut invoquer le privilège de la recherche; ces conditions sont cumulatives.

Première condition (let. a): l'entité qui utilise des données personnelles à des fins de recherche, de planification ou de statistique, doit les rendre anonymes aussitôt que la finalité du traitement le permet. On entend par rendre anonyme, toute démarche visant à empêcher l'identification des personnes concernées ou à ne rendre celle-ci possible qu'au prix d'efforts démesurés. En pratique, il arrive fréquemment que le chercheur, le planificateur ou le statisticien, bien qu'il utilise des données dépourvues de références à des personnes déterminées, n'entende néanmoins pas les rendre d'emblée anonymes, car il doit conserver la possibilité de vérifier exceptionnellement l'identité d'une personne. Lorsqu'il est confronté à de

[166] FF 1988 II 421, p. 479

telles situations, il se doit de coder ou de crypter les données. Il peut, par exemple, séparer les caractéristiques personnelles des autres données, de telle sorte qu'il ne soit plus possible de mettre en relation telle donnée avec telle personne sans passer par le numéro de référence[167].

Conformément à la lettre b, l'entité ne communique des données sensibles que sous une forme ne permettant pas d'identifier les personnes concernées. Cette modification vise à renforcer la protection des données sensibles. Cette condition est réalisée lorsque les données sont communiquées sous une forme pseudonymisée, et que la clé pour réidentifier la personne reste chez celui qui transmet les données (anonymisation factuelle)[168].

En vertu de la lettre c, l'entité qui a collecté les données doit donner son accord à leur nouvelle transmission à des tiers par le destinataire originel.

Enfin, les privilèges institués par l'article 41 sont liés à la condition que les résultats du traitement soient publiés sous une forme ne permettant pas, selon le cours ordinaire des choses, d'identifier les personnes concernées (let. d).

Le 2e alinéa énumère exhaustivement les dispositions de la loi qui ne sont pas applicables au traitement de données ne se rapportant pas à des personnes. Il s'agit d'abord du principe de la compatibilité des buts institué par l'article 35, alinéa 3 du présent projet. Etant donné que la recherche, la planification ou la statistique sont des activités sans effet direct sur les personnes concernées, il n'y a pas lieu d'interdire l'utilisation de données qui ont été collectées à de toutes autres fins (let. a). Pour la même raison, les institutions pourront traiter des données sensibles ou effectuer du profilage à des fins de statistique, de recherche ou de planification, ou encore à tout autre fin ne se rapportant pas à des personnes, sans être tenues de se conformer aux conditions spéciales instituées par l'article 36, alinéa 2 du présent projet, (let. b) pour autant que l'exigence de base légale ou de traitement nécessaire à l'accomplissement des tâches légales de l'institution publique (article 36, alinéa 1 du présent projet) soit respecté. Il n'est pas nécessaire non plus qu'ils observent les dispositions générales sur la communication de données (let. c). Il s'ensuit que la communication de données à des fins ne se rapportant pas à des personnes ne nécessite aucune base juridique supplémentaire. Il n'est pas non plus exigé que le destinataire ait absolument besoin des données pour accomplir une tâche légale, ni que la personne concernée ait donné son consentement. Cela dit, en vertu de la lettre c, l'entité qui a collecté les données doit donner son accord à leur nouvelle transmission.

[167] FF 1988 II 421, p. 480
[168] FF 2017 6565, p. 6699

Art. 43

La LIPAD contient déjà, à l'heure actuelle, à son article 43, le catalogue des fichiers (CATFICH). Selon cette disposition, la préposée cantonale ou le préposé cantonal dresse et tient à jour un catalogue des fichiers des institutions, comportant les précisions utiles sur les informations traitées, la base légale de leur traitement, leur état de validité ou la fréquence de leur mise à jour et de leur épuration, et leur accessibilité (al. 1). Les fichiers éphémères ne recensant ni données personnelles sensibles ni profils de la personnalité sont exemptés de l'enregistrement au catalogue des fichiers (al. 2). Ce catalogue est public et rendu facilement accessible (al. 3).

Du fait de la disparition de la notion de fichier et son remplacement par la notion de traitement, ce catalogue des fichiers est désormais intitulé registre des activités de traitement. L'article 43 est par ailleurs un peu remanié.

La directive (UE) 2016/680[169] et le RGPD[170] prévoient également un tel registre.

Al. 1

Comme c'est le cas à l'heure actuelle pour CATFICH, c'est la préposée cantonale ou le préposé cantonal qui dressera et tiendra à jour le registre des activités de traitement des institutions. De même, à l'instar de ce qui est prévu à l'article 43, alinéa 3 dans sa teneur actuelle, ce registre sera public et rendu facilement accessible.

Al. 2

L'alinéa 2 précise les indications minimales que doit contenir le registre.

Par *« catégories des personnes concernées »* on entend des groupes partageant les mêmes caractéristiques. Les catégories des données personnelles traitées désignent la nature des données (données sensibles, par ex.)[171].

Par *« catégories de destinataires »* On entend également par là des groupes partageant les mêmes caractéristiques (*« autorités de surveillance »*, par ex.)[172].

[169] Art. 24
[170] Art. 30
[171] FF 2017 6565, p. 6655
[172] Ibid.

La déclaration du registre des activités de traitements doit également mentionner les autres responsables du traitement, en cas de responsables du traitement conjoints, ainsi que les obligations respectives des différentes institutions responsables (voir également *supra* commentaire ad art. 36B).

La déclaration doit également indiquer l'identité et les coordonnées des sous-traitants.

Al. 3

L'alinéa 3 énumère quant à lui les indications que les institutions fournissent à la préposée cantonale ou au préposé cantonal, sur requête de ces derniers.

S'agissant du *« délai de conservation des données »*, ce délai étant lié, conformément à l'article 35, aux finalités du traitement, il n'est pas toujours possible de l'établir avec précision, d'où la mention *« dans la mesure du possible »*. S'il n'est pas possible de fournir une indication précise, le registre doit au moins indiquer les critères selon lesquels ce délai sera fixé[173].

En ce qui concerne les *« mesures visant à garantir la sécurité des données »*, le but de leur description est de faire apparaître d'éventuels manquements dans les mesures de sécurité. La mention « dans la mesure du possible » indique que cette obligation ne s'applique que si les mesures peuvent être définies de manière suffisamment concrète[174].

Si les destinataires sont à l'étranger, la préposée ou le préposé cantonal doit en outre pouvoir savoir si les conditions d'une communication à l'étranger sont remplies. La lettre g. prévoit donc que les informations communiquées doivent en tous les cas mentionner le nom de l'Etat ou de l'organisme international destinataire, et, le cas échéant, les exceptions prévues à l'article 39, alinéa 7.

Al. 4

Comme mentionné ci-dessus, à l'heure actuelle, l'article 43, alinéa 2 LIPAD prévoit que les fichiers éphémères ne recensant ni données personnelles sensibles ni profils de la personnalité n'ont pas à être déclarés dans CATFICH. Du fait de la disparition de la notion de *« fichier »* et afin de permettre au Conseil d'Etat de prévoir des exceptions à l'obligation de déclarer pour certaines catégories de traitements à des fins administratives

[173] Ibid.
[174] Ibid.

internes qui ne présentent manifestement pas de risques pour les droits des personnes concernées, l'article 43, alinéa 2 actuel est remplacé par cet alinéa.

Art. 44 et 45

Ces articles reprennent la notion du droit d'accès déjà connue dans la LIPAD actuelle, en l'adaptant à l'évolution du droit supérieur.

Art. 44

Cet article énonce les principes du droit d'accès. La nLPD[175], la Convention 108+[176], la directive (UE) 2016/680[177] et le RGPD[178] contiennent des dispositions similaires.

Le droit d'accès complète l'obligation d'informer du responsable du traitement. Il est la clé qui permet à la personne concernée de faire valoir les droits que lui octroie la loi.

Al. 1

L'alinéa 1 dispose que toute personne physique ou morale de droit privé peut demander par écrit au responsable du traitement si des données la concernant sont traitées. En effet, conformément aux travaux préparatoires de la LIPAD[179] actuelle, il est précisé que seule une personne physique ou morale de droit privé se voit conférer des droits en relation avec ses propres données personnelles. Le but de la loi n'est pas de conférer aux institutions de droit public qui lui sont soumises des droits spécifiques à cet égard. Il est dès lors précisé que ce catalogue de droits ne concerne que les personnes de droit privé.

Le droit d'accès appartient ainsi à toute personne physique ou morale de droit privé 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.

Par rapport au droit en vigueur, la justification de l'identité est transférée dans l'article 45 relatif aux modalités. Il est par ailleurs désormais fait référence au responsable du traitement et non plus au responsable LIPAD.

[175] Art. 25
[176] Art. 9 par. 1 let. b
[177] Art. 14
[178] Art. 15
[179] PL 9870, exposé des motifs, p.69 ad art. 17

Al. 2

L'alinéa 2 dispose que la personne physique ou morale de droit privé mentionnée à l'alinéa 1 reçoit les informations nécessaires à la mise en œuvre de ses droits en matière de protection des données personnelles et pour garantir la transparence du traitement. A sa demande, elle reçoit du responsable du traitement les informations listées aux lettres a à f.

Cette disposition met en lumière non seulement le lien étroit qui existe entre le droit d'accès et le devoir d'informer, mais aussi le but fondamental du droit d'accès qui est de permettre à la personne concernée de faire valoir ses droits en matière de protection des données[180]. En ce sens, cette disposition limite clairement le droit d'accès : le droit d'accès vise uniquement à aider une personne concernée à faire valoir ses droits en matière de protection des données (au moins ses droits pouvant faire l'objet d'une action en justice) et à garantir la transparence du traitement des données (p. ex. pour permettre à une personne de choisir de fournir ou non des données ou de savoir – pour sa tranquillité d'esprit – quelles données une institution publique détient à son sujet).

Les lettres a à f donnent une énumération non exhaustive des informations qui doivent être communiquées dans tous les cas à la personne concernée. La norme générale dans la phrase introductive permet subsidiairement de demander d'autres informations qui sont nécessaires pour que la personne physique ou morale de droit concernée puisse faire valoir ses droits en vertu de la LIPAD et pour garantir la transparence du traitement. Lorsqu'elle traite des quantités importantes de données sur la personne concernée, la personne tenue de fournir les renseignements doit pouvoir demander à cette dernière de préciser sur quelles données ou quelles opérations de traitement porte sa requête[181].

Al. 3

Le débiteur du droit d'accès est toujours le responsable du traitement. Le fait que celui-ci confie le traitement à un sous-traitant ne change rien à cet égard.

Lorsque la personne concernée adresse une demande d'accès directement au sous-traitant, celui-ci doit lui indiquer le nom du responsable du traitement ou transmettre sa demande à ce dernier. S'il n'est pas tenu, en pareil cas, de

[180] Voir à ce sujet l'ATF 138 III 425, consid. 5.3
[181] FF 2017 6565, p. 6683

renseigner lui-même la personne concernée, le sous-traitant ne doit pas non plus entraver l'exercice du droit d'accès[182].

Al. 4

Le droit d'accès est un droit subjectif inhérent à la personne, que même une personne qui n'a pas l'exercice des droits civils mais qui est capable de discernement peut faire valoir seule, sans avoir à requérir le consentement de son représentant légal. Le fait que ce droit est inhérent à la personne a pour conséquence que nul ne peut y renoncer par avance[183] (voir art. 44 , al. 4 du présent projet).

Art. 45

Cet article énonce les modalités du droit d'accès. Cette disposition existe déjà dans la LIPAD actuelle, mais a été légèrement remaniée, à l'instar de l'article 44.

Al. 1

La justification de l'identité figurait déjà dans l'article 44 LIPAD actuel. Elle a été regroupée avec les autres dispositions concernant les modalités du droit d'accès par souci de cohérence.

Al. 2

L'article 45 dans sa teneur actuelle prévoit que la communication des données et informations doit être faite sous une forme intelligible et, en règle générale, par écrit et gratuitement. Cette formulation a été légèrement remaniée et prévoit désormais que les renseignements sont, en règle générale, fournis par écrit sur un support physique ou électronique. En accord avec le responsable du traitement, la personne physique ou morale de droit privé concernée peut consulter ses données sur place.

Al. 3

L'article 44, alinéa 3 dans sa teneur actuelle prévoit que la satisfaction d'une demande impliquant un travail disproportionné peut être subordonnée au paiement préalable d'un émolument. De même, l'article 45 dans sa teneur

[182] FF 2017 6565, p. 6684
[183] FF 2017 6565, p. 6682

actuelle prévoit que la communication de ces données et informations doit être faite sous une forme intelligible et, en règle générale, par écrit et gratuitement. L'article 45, alinéa 3 du présent projet regroupe ces deux dispositions et prévoit désormais que le responsable du traitement fournit gratuitement les renseignements demandés. Le Conseil d'Etat peut toutefois prévoir des exceptions, notamment si la communication de l'information implique un travail disproportionné. Cette disposition est calquée sur l'article 25, alinéa 6 nLPD.

Al. 4

Cette disposition est calquée sur l'article 25, alinéa 7 nLPD et prévoit qu'à moins que des circonstances exceptionnelles ne le justifient, le responsable du traitement doit fournir les renseignements demandés dans un délai de 30 jours.

Art. 47, al. 2

Le présent projet modifie certaines lettres de l'alinéa 2.

A la lettre a, il ajoute la notion d'effacement, qui a également été ajoutée dans la liste exemplative des traitements (voir *supra* commentaire ad art. 4). Les lettres b et e sont simplement adaptées à l'inversion, dans le présent projet, des articles 35 et 36.

A toutes fins utiles, il sera rappelé que conformément aux travaux préparatoires de la LIPAD actuelle[184], le droit d'obtenir des institutions les actions sollicitées n'existe que *« sauf disposition légale contraire »*, afin de réserver notamment aussi bien les règles particulières de la loi sur les archives publiques, du 1er décembre 2000 (LArch ; B 2 15) relatives à la destruction des dossiers que celle de la loi sur la santé, en particulier l'art. 57 de cette dernière qui traite de la conservation du dossier du patient.

Art. 49

Cet article reprend l'actuel article 49 LIPAD en le modifiant.

A l'alinéa 1, suite à la suppression de la définition d'*« organe »*, ce terme a ainsi été remplacé par les termes *« responsable du traitement »*.

Par ailleurs, comme cela sera exposé plus en détail ci-après (voir *infra* commentaire ad art. 56C), la préposée cantonale ou le préposé cantonal aura

[184] PL 9870, exposé des motifs, p. 70 ad art. 17

désormais de nouveaux pouvoirs d'intervention et d'investigation, conformément aux exigences de la Convention 108+ et de la directive (UE) 2016/680. Le RGPD prévoit également ces exigences. Cela a pour conséquence que la préposée cantonale ou le préposé cantonal aura désormais le pouvoir de rendre des décisions à l'encontre des institutions.

De ce fait, par souci de cohérence de l'activité de la préposée cantonale ou du préposé cantonal, le présent projet prévoit de supprimer la procédure de recommandation de la préposée cantonale ou du préposé cantonal dans le cadre de l'article 49 LIPAD.

Les alinéas 3 à 5 sont ainsi abrogés.

L'alinéa 6 est modifié pour prévoir que l'institution statue par voie de décision dans les 30 jours sur les prétentions du requérant. La pratique a en effet démontré que l'appréciation desdites prétentions nécessite un examen approfondi qui dépasse souvent, voire toujours, les 10 jours. Comme actuellement, ce délai de 30 jours constitue un délai d'ordre.

Art. 50

Cet article reprend l'actuel article 50 LIPAD en le modifiant légèrement.

Al. 1

La LIPAD actuelle prévoit déjà que des responsables ayant une formation appropriée et les compétences utiles doivent être désignés au sein des institutions, pour y garantir une correcte application de la présente loi. Les travaux préparatoires de la LIPAD actuelle précisaient à cet égard que les responsables des institutions sont la cheville ouvrière du nouveau dispositif. Ce constat renforce la nécessité de mettre un soin tout particulier dans la désignation des responsables et leur organisation, afin de faciliter autant que faire se peut l'efficacité de leur action. On ne saurait ici définir de manière trop rigide les compétences et le niveau de formation attendu des futurs responsables, tant les institutions ont des moyens en personnel et en budget qui peuvent se révéler différents. Poser des exigences trop élevées quant à la formation appropriée des responsables alors qu'une petite institution ne peut immédiatement les satisfaire serait contre-productif. En revanche, la nécessité d'une formation continue et l'appui de la préposée cantonale ou du préposé cantonal à cet égard seront des atouts supplémentaires auxquels chaque institution pourra recourir[185].

[185] PL 9870, exposé des motifs, p. 74 ad art. 21

La terminologie est toutefois adaptée au droit fédéral, les responsables LIPAD étant désormais dénommés *« conseillères et conseillers à la protection des données et à la transparence »*, à l'instar de la nLPD[186] et du projet d'OLPD[187]. Cette fonction est également prévue dans la directive (UE) 2016/680[188] et le RGPD, sous l'appellation *« délégué à la protection des données »*. Elle est également mentionnée dans le rapport explicatif de la Convention 108+[189].

Al. 2

Cet alinéa est repris de la LIPAD actuelle et a été complété suite à la proposition d'inclure la Cour des comptes dans les institutions soumises à la LIPAD.

Al. 3

Cet alinéa est repris de la LIPAD actuelle et a été complété suite à l'alinéa 2 ci-dessus.

S'agissant plus spécifiquement de la lettre h, les travaux préparatoires de la LIPAD actuelle indiquaient à cet égard que cette lettre précise que ce sont toutes les *« instances supérieures »* des établissements et corporations de droit public cantonaux et communaux qui sont visées par la nouvelle disposition, ce qui englobe l'ensemble des organes supérieurs, qu'ils soient de type exécutif, délibératif ou d'une autre nature[190].

Al. 6

Cet alinéa a été modifié pour tenir compte de la nouvelle terminologie de l'article 50.

Art. 51

Cet article reprend l'actuel article 51 LIPAD en le complétant et en le modifiant.

[186] Art. 10, al. 4
[187] Art. 27 à 30
[188] Art. 32 à 34
[189] Rapport explicatif de la Convention 108+, ch. 87 ad art. 10
[190] PL 9870, exposé des motifs, p. 75 ad art. 21

Al. 1 et 2

Ces alinéas introduisent la notion de conseillère et conseiller LIPAD, et en décrivent la fonction de manière générale. Ainsi, ces alinéas précisent que les conseillères et conseillers LIPAD:

- sont les interlocuteurs des personnes concernées et de la préposée cantonale ou du préposé cantonal pour tout ce qui a trait au traitement des données personnelles et à la transparence de leur institution publique (al. 1);
- assument une fonction de conseil et de soutien (al. 2);
- sont associés de manière appropriée aux activités de traitement (al. 2).

Al. 3

Cet alinéa vient préciser les deux premiers alinéas et les tâches accomplies par les conseillères et conseillers LIPAD.

Outre la fonction de conseil et soutien aux membres de leur institution publique en matière de protection des données (let. a), ils donnent également à ces derniers les instructions utiles sur le traitement des données personnelles nécessaires à l'accomplissement de leurs tâches légales ou des demandes d'accès aux documents en matière de transparence (let. b ; cette disposition est reprise de l'article 51, alinéa 2 lettre b de la LIPAD actuelle). Ils doivent également concourir à l'établissement de l'analyse d'impact relative à la protection des données (let. c; voir également *supra* commentaire ad art. 37B concernant l'analyse d'impact) et communiquer à la préposée cantonale ou au préposé cantonal la liste des activités de traitement de l'institution publique au sens de l'article 43 du présent projet, ainsi que ses mises à jours particulières (let. d ; voir également *supra* commentaire ad art. 43 concernant le registre des activités de traitement). Enfin, ils sont chargés d'annoncer à la préposée cantonale ou au préposé cantonal la violation de la sécurité des données pour le compte du responsable du traitement (let. d ; voir également *supra* commentaire ad art. 37C).

Al. 4

Cette disposition est reprise de l'article 51, alinéa 2 LIPAD actuelle.

Al. 5

Cette disposition est reprise de l'article 51, alinéa 1 LIPAD actuelle.

Art. 52, al. 2 et 3

Ces alinéas sont repris de l'article 56, alinéas 6 et 7 LIPAD actuels et regroupés dans cet article dans la mesure où ils concernent également la thématique de la *« coordination »*.

Art. 55A

Cette disposition est calquée sur l'article 48 nLPD.

Elle prévoit que la préposée cantonale ou le préposé cantonal doit s'assurer, par des mesures de contrôle appropriées portant notamment sur la sécurité des données personnelles, du respect et de la bonne application des dispositions de la présente loi en son sein.

Art. 56 et 56A

Pour faciliter la lecture, et dans la mesure où les compétences de la préposée cantonale ou du préposé cantonal en matière de protection des données ont été étoffées, le présent projet propose de séparer l'article 56 LIPAD actuel en 2 volets, l'un en matière d'information du public et l'accès aux documents (art. 56), l'autre en matière de protection des données (art. 56A).

Art. 56

Cet article reprend la teneur de l'article 56, alinéas 1 et 2 LIPAD actuels. Seule une modification formelle a été apportée à ces derniers, du fait que cet article ne concerne désormais plus que le volet de l'information du public et l'accès aux documents.

Art. 56A

Cet article reprend la teneur de l'article 56, alinéa 3 de la LIPAD actuelle. Par parallélisme avec l'article 56, alinéa 1 du présent projet, l'alinéa 1 de l'article 56A du présent projet introduit, de manière générale, la mission de la préposée cantonale ou du préposé cantonal en matière de protection des données.

Elle adapte par ailleurs la terminologie aux modifications apportées dans le présent projet par rapport à la loi actuelle (disparition de la notion de *« fichier »* au profit de celle de *« traitement »*, voir également *supra* commentaire ad art. 4; remplacement des *« responsables »* en matière de

protection des données par les *« conseillères et conseillers en matière de protection des données »*, voir également *supra* commentaire ad art. 50).

Art. 56B

Cette disposition prévoit de renforcer les moyens d'intervention de la préposée cantonale ou du préposé cantonal, conformément aux nouveaux standards des lois de protection des données, que ce soit la nLPD[191], la Convention 108+[192], la directive (UE) 2016/680[193] ou encore le RGPD[194].

Al. 1 et 4

En vertu de l'alinéa 1, la préposée cantonale ou le préposé cantonal peut effectuer, d'office ou sur dénonciation, un contrôle auprès d'une institution publique ou d'un sous-traitant afin de vérifier qu'ils respectent les dispositions de protection des données.

La préposée cantonale ou le préposé cantonal peut décider librement des contrôles qu'il opère et de la suite à donner à une dénonciation (al. 1, deuxième phrase), à l'instar du préposé fédéral qui peut renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance ou s'il considère que la fourniture de conseils au responsable du traitement concerné peut constituer une mesure suffisante pour remédier à une situation en soi peu problématique[195].

Le dénonciateur peut être un tiers ou la personne concernée. Toutefois, même dans le cas où le dénonciateur est la personne concernée, cette dernière n'aura pas qualité de partie à la procédure (cf. art. 56D, al. 2, a contrario), contrairement aux cas des articles 44, 47 et 49 LIPAD. La préposée cantonale ou le préposé cantonal sera toutefois tenu de l'informer de la suite donnée à sa dénonciation (al. 4).

Al. 2 et 3

Ces alinéas traitent du devoir de collaboration des institutions et des sous-traitants et de la problématique du secret de fonction, et autres secrets institués par la loi, qui y est liée.

---

[191] Art. 49 nLPD
[192] Art. 15, par. 2 let. a à d
[193] Art. 47, par. 2
[194] Art. 58, par. 2
[195] FF 2017 6565, p. 6706

La préposée cantonale ou le préposé cantonal peut ainsi notamment demander des renseignements, exiger la production de documents, procéder à des inspections et se faire présenter des traitements de donner. Il peut également recourir, au besoin, à des experts dans les domaines techniques (al. 2).

Le secret de fonction ne peut pas lui être opposé dans ce cadre. Les autres secrets institués par la loi sont toutefois réservés (al. 3). Cet alinéa est calqué sur l'article 131 de la Constitution de la République et canton de Genève, du 14 octobre 2012 (Cst-GE ; A 2 00), applicable à la Cour des comptes, ainsi que sur les articles 201A, alinéa 7 et 230H, alinéa 3 de la loi portant règlement du Grand Conseil de la République et canton de Genève, du 13 septembre 1985 (LRGC ; B 1 01), applicables à la Commission de contrôle de gestion et aux Commissions d'enquêtes parlementaires.

Art. 56C

Cette disposition a été inspirée de la nLPD[196], qui met en œuvre la directive (UE) 2016/680[197] et donne suite aux recommandations des évaluateurs Schengen de conférer des compétences décisionnelles à la préposée cantonale ou au préposé cantonal[198], qui ont recommandé de renforcer les pouvoirs d'exécution des autorités cantonales chargées de la protection des données en les habilitant à prendre directement des décisions juridiquement contraignantes. La Convention 108+ prévoit également que les autorités de contrôle disposent du pouvoir de rendre des décisions relatives aux violations des dispositions de la présente Convention et peuvent, notamment, infliger des sanctions administratives[199].

Le RGPD[200] contient une disposition similaire, qui énumère par ailleurs toutes les mesures correctrices que l'autorité de contrôle est habilitée à prendre. L'octroi d'une compétence décisionnelle à l'autorité de surveillance est un élément déterminant au sens de l'article 45 RGPD pour décider du

196 Art. 51

197 Art. 47, par. 2

198 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, du 8 mars 2019

199 Art. 15, par. 2 let. c

200 Art. 58, par. 2

maintien de la décision d'adéquation de la Commission européenne en faveur de la Suisse[201].

L'article 56C laisse une grande marge de manœuvre à la préposée cantonale ou au préposé cantonal. En effet, cette disposition ne l'oblige pas à prendre des mesures administratives, mais lui donne la faculté de le faire.

L'article 56C contient deux catégories de mesures.

Al. 1 et 2

La première catégorie prévoit un catalogue de mesures contre des traitements de données contraires à des dispositions de protection des données. Le principe de base de cette réglementation est le respect du principe de proportionnalité. Ainsi, au lieu d'ordonner la cessation du traitement, la préposée cantonale ou le préposé cantonal peut ordonner sa modification et limiter la mesure à la partie du traitement problématique.

Al. 3

La seconde catégorie concerne des cas de non-observation de prescriptions d'ordre ou de devoirs à l'égard de la personne concernée. Parmi les compétences décisionnelles qui sont attribuées à la préposée cantonale ou au préposé cantonal, celui-ci peut par exemple ordonner à l'institution publique de se conformer à son devoir d'informer lors de la collecte des données, conformément à l'article 38 du présent projet, ou de procéder à une analyse d'impact relative à la protection des données personnelles au sens de l'article 37B du présent projet. La liste de l'alinéa 3 n'est pas exhaustive.

Suivant en cela le choix fait par la Confédération pour la nLPD, la préposée cantonal ou le préposé cantonal ne disposera pas du pouvoir de prononcer des sanctions administratives à l'encontre des institutions[202].

Art. 56D

Cette disposition prévoit que la procédure est régie par la loi sur la procédure administrative, du 12 septembre 1985 (al. 1).

L'alinéa 2 prévoit que l'institution publique visée par une décision de la préposée cantonale ou du préposé cantonal a qualité pour recourir contre

[201] FF 2017 6565, p. 6707
[202] FF 2017 6565, p. 6589

celle-ci. Par conséquent, seuls celles-ci peuvent recourir contre les mesures prononcées contre eux par la préposée cantonale ou le préposé cantonal.

La personne concernée n'a pas qualité de partie à la procédure, même si la préposée cantonale ou le préposé cantonal a ouvert l'enquête sur dénonciation de celle-ci (voir *supra* commentaire ad art. 56B). Dans la mesure où la personne concernée entend faire valoir des prétentions d'une institution publique responsable du traitement, elle doit procéder selon l'article 47 du présent projet, en recourant le cas échéant contre la décision de l'institution publique responsable du traitement auprès de la Chambre administrative de la Cour de justice.

Art. 56E

Cette disposition, nouvelle, règle la collaboration entre les autorités cantonales, fédérales et étrangères chargées de la protection des données.

La Convention 108+[203] prévoit également que les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs fonctions et l'exercice de leurs pouvoirs, notamment: a. en s'accordant mutuellement une assistance par l'échange d'informations pertinentes et utiles et en coopérant entre elles, à condition qu'en ce qui concerne la protection des données à caractère personnel toutes les règles et garanties de la présente Convention soient respectées; b. en coordonnant leurs investigations ou interventions, ou en menant des actions conjointes; c. en fournissant des informations et des documents sur leur droit et sur leurs pratiques administratives en matière de protection des données.

La directive (UE) 2016/680[204] et le RGPD[205] contiennent des dispositions similaires.

Art. 60

Conformément à la technique législative arrêtées lors de la dernière réforme de la juridiction administrative, il n'y a lieu d'inscrire dans les lois cantonales, au chapitre des voies de droit, que ce qui est spécifique à la matière traitée, dès lors que les voies de droit en matière administrative se trouvent régies de façon générale par la loi sur l'organisation judiciaire (LOJ ; E 2 05) et par la loi sur la procédure administrative (LPA ; E 5 10).

[203] Art. 17
[204] Art. 50
[205] Art. 61

En l'occurrence, le contentieux relatif à l'accès aux documents présente quelques particularités, raison pour laquelle l'article 60 LIPAD a en son temps été adopté. Cela étant, par souci didactique, une modification formelle de son titre est proposée afin de refléter plus exactement son contenu. Elle vise à remplacer le titre "Objet du recours" par "Recours en matière d'accès aux documents". Le contenu de la disposition est en revanche inchangé.

Art. 68, al. 8

Cet alinéa est calqué sur l'article 69 nLPD. Il prévoit, à l'instar du droit fédéral, que les dispositions relatives à la protection des données dès la conception et par défaut et celles relatives aux analyses d'impact ne s'appliquent pas aux traitements qui ont débuté avant l'entrée en vigueur du présent projet, pour autant que les finalités du traitement restent inchangées et que de nouvelles données ne soient pas collectées.

Modifications à d'autres lois

1. Loi sur la Haute école spécialisée de Suisse occidentale - Genève

Est introduite, au sein de la loi régissant la HES-SO Genève, une base légale spécifique relative au traitement de données personnelles, y compris sensibles, et au profilage, par ladite institution, dans la mesure nécessaire à la réalisation de sa mission de recherche scientifique fondamentale et appliquée.

Il est relevé qu'un tel ajout a été recommandé par le Préposé cantonal à la protection des données et à la transparence.

Les dispositions de la loi fédérale relative à la recherche sur l'être humain, tout comme celles de la LIPAD, ainsi que celles de leurs règlementations d'application respectives, sont toutefois réservées.

2. Loi sur l'Université

Est introduite, au sein de la loi régissant l'Université de Genève, une base légale spécifique relative au traitement de données personnelles, y compris sensibles, et au profilage, par ladite institution, dans la mesure nécessaire à la réalisation de sa mission de recherche scientifique fondamentale et appliquée.

Il est relevé qu'un tel ajout a été recommandé par le Préposé cantonal à la protection des données et à la transparence.

Les dispositions de la loi fédérale relative à la recherche sur l'être humain, tout comme celles de la LIPAD, ainsi que celles de leurs règlementations d'application respectives, sont toutefois réservées.

3. Loi sur la surveillance de l'Etat

L'inclusion de la Cour des comptes parmi les institutions soumises à la LIPAD nécessite de modifier l'article 34 LSurv afin de préciser les contours des modalités du volet transparence dans le cadre de la révision des états financiers individuels et consolidés de l'Etat de Genève.

L'article 34 LSurv est ainsi modifié afin de prévoir que les communications écrites complémentaires aux états financiers individuels et consolidés de l'Etat de Genève ne peuvent pas faire l'objet d'une demande d'accès aux documents au sens de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001. La même règle s'applique aux documents relatifs à d'autres entités reçus par la Cour des comptes dans le cadre de la révision des états financiers individuels et consolidés de l'Etat de Genève.

4. Loi sur les établissements publics médicaux

Est introduite, au sein de la loi sur les établissements publics médicaux, une base légale spécifique relative au traitement de données personnelles, y compris sensibles, et au profilage, par les HUG, dans la mesure nécessaire à la réalisation de leur mission de recherche médicale fondamentale et clinique.

Un tel ajout été recommandé par le Préposé cantonal à la protection des données et à la transparence pour ce qui concerne l'Université de Genève et la HES-SO Genève. Cet ajout se justifie également pour ce qui concerne les HUG, la recherche faisant partie de leurs activités (art. 2, al. 2, let. b LEPM) et la LEPM ne contenant pas, à ce jour, de dispositions spécifiques sur le traitement de données personnelles sensibles ou sur le profilage dans le cadre d'une étude médicale.

Les dispositions de la loi fédérale relative à la recherche sur l'être humain tout comme celles de la LIPAD, ainsi que celles de leurs règlementations d'application respectives, sont toutefois réservées.

Au bénéfice de ces explications, nous vous remercions, Mesdames et Messieurs les Députés, de réserver un bon accueil au présent projet de loi.

Annexes :
1) *Préavis financier*
2) *Planification des charges et revenus de fonctionnement découlant du projet*
3) *Planification des dépenses et recettes d'investissement découlant du projet, le cas échéant*
4) *Avis du préposé cantonal lorsque le projet de loi a un impact en matière de transparence ou de protection des données personnelles*
5) *...*