Rapport

Date de la séance du CE : 13 novembre 2024
Direction : Direction de l'intérieur et de la justice
N° d'affaire : 2019.JGK.647
Classification : Non classifié

Loi cantonale sur la protection des données (LCPD)

Table des matières

1. Synthèse 3

2. Contexte 4
2.1 Conséquences de l'évolution du droit européen sur la Suisse 4
2.2 Mise en œuvre au niveau fédéral 4
2.3 Mise en œuvre au niveau cantonal 5

3. Caractéristiques de la nouvelle réglementation 5
3.1 Principe 5
3.2 Champ d'application 6
3.3 Actualisation du catalogue des données sensibles 6
3.4 Dispositions sur la transparence 6
3.5 Registre des fichiers et registre des activités de traitement 7
3.6 Domaine de surveillance 8
3.7 Systématique du droit 8
3.8 Révision d'autres lois 9
3.8.1 Révision de lois spéciales 9
3.8.2 Loi du 7 mars 2022 sur l'administration numérique (LAN) 10
3.8.3 Loi du 12 septembre 1985 sur l'établissement et le séjour des Suissesses et des Suisses(LES) et loi du 9 décembre 2019 portant introduction de la loi fédérale sur l'asile et de la loi fédérale sur les étrangers et l'intégration (Li LFAE) 10
3.8.4 Loi du 20 juin 1995 sur l'organisation du Conseil-exécutif et de l'administration (loi d'organisation, LOCA) 10
3.9 Dispositions écartées 10
3.9.1 Ordonnance exploratoire 10
3.9.2 Conseillère ou conseiller à la protection des données 11
3.9.3 Disposition relative à la responsabilité 11

4. Forme de l'acte législatif 12

5. Droit comparé 12
5.1 Canton d'Argovie 12
5.2 Canton de Saint-Gall 13
5.3 Canton de Zurich 13
5.4 Canton de Lucerne 13
5.5 Résumé 14

6. Mise en œuvre, évaluation 14

7. Commentaire des articles 14
7.1 Dispositions générales 14
7.2 Traitement de données personnelles 25
7.3 Obligations des autorités et des tiers mandatés 42
7.4 Droits de la personne concernée 50
7.5 Autorités de protection des données 54

7.6 Procédure et protection juridique 67
7.7 Dispositions d'exécution 68
7.8 Dispositions transitoires et dispositions finales 69
7.8.1 Dispositions transitoires 69
7.9 Modifications d'autres actes législatifs 71
7.9.1 Loi du 19 février 1986 sur la protection des données (LCPD) 71
7.9.2 Modification indirecte de la loi du 7 mars 2022 sur l'administration numérique (LAN) 71
7.9.3 Modification indirecte de la loi du 12 septembre 1985 sur l'établissement et le séjour des Suissesses et des Suisses (LES) et de la loi du 9 décembre 2019 portant introduction de la loi fédérale sur l'asile et de la loi fédérale sur les étrangers et l'intégration (Li LFAE) 72
7.9.4 Modification indirecte de la loi du 20 juin 1995 sur l'organisation du Conseil-exécutif et de l'administration (loi d'organisation, LOCA) 72
7.9.5 Modification indirecte de la loi du 10 février 2019 sur la police (LPol) 73
7.9.6 Modification indirecte de la loi du 9 mars 2021 sur les programmes d'action sociale (LPASoc) et de la loi cantonale du 10 juin 2020 sur les jeux d'argent (LCJar) 73
7.9.7 Adaptations liées au nouveau titre de l'acte (modifications indirectes) 73
7.9.8 Adaptation de la terminologie française concernant les données sensibles (modifications indirectes) 74

8. Place du projet dans le programme gouvernemental de législature (programme législatif) et dans d'autres planifications importantes 76

9. Répercussions financières 76

10. Répercussions sur le personnel et l'organisation 76

11. Répercussions sur les communes 77

12. Répercussions sur l'économie 77

13. Résultat de la procédure de consultation 77
13.1 Champ d'application pour les personnes morales 77
13.2 Définitions 78
13.3 Base juridique pour le traitement des données personnelles 79
13.4 Communication à l'étranger: variante proposée 80
13.5 Conservation, destruction et archivage 81
13.6 Analyse des risques en cas de traitements répétés envisagés 81
13.7 Fichiers et obligation d'inscrire au registre 81
13.8 Obligations d'annoncer en cas de violations de la sécurité des données 82
13.9 Centralisation des autorités de protection des données 82
13.10 Mesures administratives 83
13.10.1 Voie de droit 83
13.11 Compétence décisionnelle à l'égard des tribunaux et du Ministère public 84

14. Proposition 84

1. Synthèse

Le droit à la protection des données est un droit fondamental. La Constitution du canton de Berne du 6 juin 1993 (ConstC)[1] concrétise, à l'article 18, le droit à l'autodétermination en matière d'information, qui découle de l'article 13, alinéa 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.)[2], comme droit à la protection des données. L'ancrage constitutionnel révèle toute l'importance qui est accordée à ce droit; son origine repose sur la peur qu'inspire un contrôle des individus par l'État. Le droit fondamental à la protection des données est mis en œuvre conformément aux règles constitutionnelles lorsque les autorités procèdent à un traitement adéquat et transparent des données personnelles, ainsi que lorsque les personnes concernées savent leurs données traitées et peuvent agir contre des traitements illicites.

Les autorités fédérales et les personnes privées sont soumises à la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[3]; s'agissant des autorités cantonales et communales, le traitement de données personnelles est régi par leur propre législation sur la protection des données.

Le droit de la protection des données est transversal, donc lié à plusieurs branches du droit. Par conséquent, la loi du 19 février 1986 sur la protection des données (LCPD)[4] règle la matière en général (principes de traitement, droits des personnes concernées, surveillance, etc.). Ses principes sont mis en œuvre dans une loi spéciale (c'est-à-dire composée de règles concrètes et spécifiques que l'on appelle aussi droit matériel concernant la protection des données).

En application du développement de l'acquis de Schengen, la Confédération et les cantons sont tenus de concevoir leur droit en matière de protection des données pour qu'il soit conforme au système de l'Union européenne. Le projet apporte aux bases légales cantonales les adaptations nécessaires afin qu'elles correspondent au droit européen et à la législation fédérale: l'exclusion générale de l'application de la loi cantonale sur la protection des données dans les procédures pendantes d'administration de la justice doit être abrogée. Doivent seuls rester exclus du champ d'application de cette loi le traitement concret de données personnelles et les droits des personnes concernées. De ce fait, la sécurité des données, par exemple, doit être garantie en tant que principe de protection des données dans les procédures judiciaires, les procédures de justice administrative et les cas soumis à des prescriptions procédurales particulières. Les activités administratives des autorités concernées sont aussi régies par la loi cantonale sur la protection des données. La révision est par ailleurs l'occasion d'étoffer le catalogue des données sensibles (anciennement désignées comme «données particulièrement dignes de protection» et «données personnelles particulièrement dignes de protection»). Les informations sur l'appartenance syndicale ou ethnique, celles d'ordre génétique ou biométrique ainsi que l'indication de poursuites ou sanction administratives se joignent aux catégories déjà existantes. Les obligations des autorités relevant de l'information et de la communication sont étendues et les droits des personnes concernées sont plus clairement définis. La charge pesant sur les autorités est réduite dans la mesure où le registre des fichiers connaît une limitation.

Un autre point important de la révision concerne le statut et l'indépendance des autorités de protection des données. Pour que les exigences techniques puissent être satisfaites et que la charge incombant aux communes soit allégée, la surveillance est dans une large mesure centralisée par rapport au modèle fédéraliste auquel elle obéissait jusque-là. Conformément aux standards européens élevés, les autorités de surveillance restantes auront désormais un pouvoir décisionnel. Il faut d'ailleurs souligner que la loi cantonale sur la protection des données abandonne la notion d'autorités de surveillance, désormais elles seront désignées sous le nom

[1] RSB 101.1
[2] RS 101
[3] RS 235.1
[4] RSB 152.04

d'autorités de protection des données. Le changement d'appellation reflète clairement le fait que ces autorités sont avant tout là pour conseiller, guider et former, plutôt que pour contrôler et sanctionner.

Les modifications, nombreuses, sont à la fois d'ordre matériel et systématique; elles impliquent une révision totale de la loi cantonale sur la protection des données.

2. Contexte

2.1 Conséquences de l'évolution du droit européen sur la Suisse

Le 27 avril 2016, le Parlement européen et le Conseil de l'Union européenne ont adopté une réforme du droit en matière de protection des données en édictant deux actes législatifs: le règlement (UE) 2016/679 (ci-après: règlement général sur la protection des données)[5] et la directive (UE) 2016/680[6]. Le 10 octobre 2018, le Conseil de l'Europe a en outre adopté le protocole[7] portant amendement à la convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après: STE n° 108+). Ratifié le 19 juin 2020 par l'Assemblée fédérale[8], le protocole d'amendement reprend dans une large mesure le contenu de la directive (UE) 2016/680, sans toutefois entrer autant dans le détail.

Pour la Suisse, la directive (UE) 2016/680 constitue un développement de l'acquis de Schengen. Elle est donc obligée d'adapter son ordre juridique en fonction de ce texte. La notification date du 1er août 2016. Le délai de deux ans pour reprendre la teneur de l'acte dans le droit suisse expirait donc le 1er août 2018. Dans le canton de Berne, la transposition a eu lieu par l'édiction de l'ordonnance du 4 juillet 2018 portant introduction de la directive (UE) 2016/680 relative à la protection des données à caractère personnel (OiDPD)[9].

En dehors de la coopération instaurée par Schengen, la Suisse est considérée comme un État tiers. Le règlement général sur la protection des données ne fait pas partie de l'acquis de Schengen. Par conséquent, il ne doit en principe pas être repris. Toutefois, un échange de données personnelles entre un État tiers et un État membre de l'Union européenne n'est possible que si l'État tiers garantit un niveau adéquat de protection. Ce niveau doit être confirmé par une décision de l'Union européenne. À l'avenir, le droit suisse sera jugé à l'aune du contenu du règlement général sur la protection des données. La Suisse peut remplir les exigences requises en mettant en œuvre le protocole d'amendement STE n° 108+ étant donné qu'on a veillé à l'adéquation du niveau de protection lors de son élaboration.

2.2 Mise en œuvre au niveau fédéral

Les Chambres fédérales ont adopté la révision totale de la loi fédérale sur la protection des données (LPD) le 25 septembre 2020[10]. La révision a permis d'adapter la législation suisse aux normes européennes de la directive (UE) 2016/680 et au protocole d'amendement STE n° 108+. Elle est entrée en vigueur le 1er septembre 2023. À cette date, la loi sur la protection des données Schengen[11], qui garantissait l'acquis de Schengen, a été abrogée.

[5] 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 (règlement général sur la protection des données)
[6] 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
[7] FF 2020, p. 577
[8] FF 2020, p. 5559
[9] RSB 152.043
[10] FF 2020, p. 7397
[11] Loi fédérale du 28 septembre 2018 sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (loi sur la protection des données Schengen, LPDS)

2.3 Mise en œuvre au niveau cantonal

Au niveau cantonal, la révision du droit de la protection des données vise à remplir les exigences que posent en la matière la directive (UE) 2016/680 et le protocole d'amendement STE nº 108+ afin que les conditions d'une décision d'adéquation soient réunies. La portée des interventions nécessaires au niveau des cantons a été évaluée par le groupe de travail concernant la protection des données de la Conférence des gouvernements cantonaux (CdC). À l'instar de celles des autres cantons, la présente révision se fonde sur le guide pratique rédigé par ce groupe de travail (guide pratique CdC).

Le délai pour la transposition de la directive (UE) 2016/680 dans le droit national expirait en août 2018 déjà, c'est-à-dire trop tôt pour que la procédure législative ordinaire puisse aboutir. Par conséquent, les dispositions requises par la directive (UE) 2016/680 et par le protocole d'amendement STE nº 108+ ont été introduites dans le droit cantonal au moyen d'une ordonnance urgente. La validité de l'ordonnance en question (OiDPD) est limitée et doit être prolongée de trois ans avant de pouvoir être intégrée au droit ordinaire par l'entrée en vigueur de la révision, et donc abrogée.

La révision est aussi l'occasion d'autres modifications nécessaires liées

- à la mise en œuvre de la motion 224-2016 (Vogt) «Assouplissement raisonnable de la protection des données»,
- à la requête de la Commission de gestion du Grand Conseil (CGes) concernant les dispositions relatives à la surveillance et à l'élection de la déléguée ou du délégué à la protection des données et
- aux questions de compétences entre les autorités communales et l'autorité cantonale de protection des données.

3. Caractéristiques de la nouvelle réglementation

3.1 Principe

L'adaptation de la législation au droit européen est une plus-value. Les principales nouveautés sont décrites ci-dessous.

- Les principes imposés au regard de la protection des données doivent être appliqués par les tribunaux et le Ministère public, sauf dans les cas que le droit européen admet.
- Le profilage à risque élevé est introduit.
- Le contrôle préalable est complété par un autre instrument: l'analyse d'impact relative à la protection des données personnelles.
- La transparence est améliorée grâce à des obligations d'informer étendues lors de la collecte de données personnelles et grâce à des obligations d'annoncer en cas de violation de la protection des données, à quelques exceptions près, permises par la législation européenne.

Le projet législatif, en plus de l'harmonisation avec le droit européen, tient aussi compte de la motion Vogt. Cette motion charge le Conseil-exécutif, d'une part, d'assouplir et de simplifier les prescriptions en matière de protection des données pour les autorités cantonales et communales, en particulier pour les aspects juridiques et organisationnels ainsi que, d'autre part, de procéder aux adaptations juridiques nécessaires et de les mettre en œuvre. Les prescriptions européennes obligent le canton de Berne à adopter dans son droit certains instruments, entravant ainsi l'assouplissement que prônait la motion. Afin de satisfaire malgré tout aux exigences

de cette dernière, le canton de Berne applique avec mesure le droit européen et prévoit des exceptions là où la législation européenne le permet. Il est toutefois inévitable de concevoir des règles plus strictes notamment en ce qui concerne la transparence.

L'organe de surveillance cantonal change de nom et devient l'autorité cantonale de protection des données. Son cahier des charges comprend diverses tâches de surveillance relevant préalablement des communes, qui connaissent ainsi un allégement aux plans organisationnel et technique.

3.2 Champ d'application

La loi sur la protection des données s'applique à chaque traitement de données personnelles effectué par des autorités, qu'elles concernent des personnes physiques ou morales. Dans le cas des personnes morales, certaines exceptions sont toutefois prévues (art. 3, al. 1, lit. *b* P-LCPD).

Jusqu'ici, le droit prévoyait une exception de principe pour l'application de la loi sur la protection des données dans les procédures pendantes devant les juridictions civile, pénale et de droit administratif. Or cette exception n'est plus possible au vu des prescriptions européennes. Le traitement de données personnelles et les droits des personnes concernées doivent toutefois continuer d'être régis par le droit de procédure applicable dans les cas concrets. Naturellement, les autorités de ces domaines sont quand même tenues de respecter les principes de la protection des données. Il leur incombe par exemple de garantir la sécurité des données, indépendamment de tout traitement de données personnelles dans le cadre d'une procédure concrète. En outre, l'autorité cantonale de protection des données exerce sur elles la surveillance dans la mesure où elles sont assujetties à la loi sur la protection des données. Elle a aussi le pouvoir de décider de mesures administratives à l'encontre des tribunaux et du Ministère public dès lors que les conditions d'application de la loi sur la protection des données sont réunies.

3.3 Actualisation du catalogue des données sensibles

Le traitement de certaines données – les données sensibles – porte de par la loi gravement atteinte au droit fondamental à la protection des données. Elles étaient auparavant normées dans un article séparé; le projet se propose de les définir au même endroit que les autres notions. La nouvelle systématique reprend la structure du droit fédéral. De plus, le catalogue doit être complété conformément à la législation européenne et à la révision de la loi fédérale sur la protection des données. Les données concernant l'appartenance à un syndicat sont explicitement mentionnées, alors qu'elles étaient jusqu'à présent implicitement comprises dans les opinions idéologiques ou politiques. Le catalogue s'étoffe également d'autres catégories comme l'origine ethnique, les poursuites ou sanctions administratives et les indications génétiques et biométriques.

3.4 Dispositions sur la transparence

En vertu de la directive (UE) 2016/680 et du protocole d'amendement STE n° 108+, les autorités ont de nouvelles obligations.

- Une analyse d'impact relative à la protection des données personnelles est prévue comme nouvel outil obligatoire.
- Les devoirs d'informer sont étendus.

- Les violations de la sécurité des données doivent être signalées, dans certains cas, aux personnes concernées.

Tout n'est pas là absolument inédit. Certes, le droit cantonal en vigueur ne prévoit aucun examen visant à établir si un traitement expose vraisemblablement la personne concernée à un risque élevé donnant lieu à une analyse d'impact relative à la protection des données personnelles, mais il connaît l'obligation pour les autorités de soumettre à l'autorité de surveillance certains projets présentant des risques particuliers en vue de sa prise de position (contrôle préalable; art. 17a LCPD). L'analyse d'impact est donc comprise dans l'obligation de procéder à un contrôle préalable. Par ailleurs, l'analyse de la sûreté de l'information et la protection des données (SIPD) menée dans le cadre de l'utilisation des technologies de l'information et de la télécommunication (TIC) par l'administration cantonale, conformément à la législation du canton en vigueur, correspond pour l'essentiel à une analyse d'impact.

S'agissant du devoir d'informer, il existe déjà aujourd'hui lors de l'acquisition de données personnelles dans les cas où les personnes concernées adressent une demande à l'autorité ou que des données personnelles sont recueillies systématiquement, notamment au moyen de questionnaires (art. 9, al. 4 LCPD). Les dispositions européennes permettent des exceptions à l'obligation d'informer. Le canton de Berne entend en faire usage pour mettre en œuvre la motion Vogt.

Une nouvelle base légale doit en revanche être créée pour le volet sur la violation de la sécurité des données. Il s'agit de fixer dans la loi l'obligation d'annoncer à l'autorité de protection des données toute violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personne concernée. Le droit cantonal de la protection des données propose plusieurs instruments devant empêcher de telles violations (analyse d'impact relative à la protection des données personnelles, contrôle préalable, mesures visant la sécurité de l'information, etc.). Il est donc possible de partir du principe que des incidents du genre ne se produiront que rarement. Si malgré tout la sécurité des données se trouvait violée, la charge qui en découlerait pourrait s'avérer, selon les circonstances, imposante.

3.5 Registre des fichiers et registre des activités de traitement

Le registre des fichiers de données continuera d'être tenu, mais son contenu sera allégé. Seuls devront y être inscrits les fichiers contenant des données sensibles. Il s'agit là d'une simplification par rapport aux dispositions en vigueur. La charge de travail que génère la tenue du registre est très lourde et a été critiquée. En vue de la mise en œuvre de la motion Vogt, il y a donc lieu de limiter les éléments figurant au registre. Du strict point de vue de la protection des données, la limitation aux seuls fichiers contenant des données sensibles n'a rien de réjouissant, puisqu'elle contrevient à l'exigence de transparence des traitements. Seules celles et ceux qui savent quelles données personnelles les concernant sont traitées peuvent faire valoir des prétentions qui découlent du droit fondamental à la protection des données. Les personnes auront certes toujours la possibilité de demander à l'autorité si des données personnelles les concernant sont traitées, mais il n'existera plus de saisie centralisée pour l'ensemble des fichiers.

Pour le reste, l'article 24 de la directive (UE) 2016/680 exige des autorités opérant dans les domaines de la justice et de la police qu'elles tiennent un registre des activités de traitement. Cette exigence doit être transposée dans la législation cantonale en matière de protection des données. Le Conseil-exécutif détermine le contenu du registre par voie d'ordonnance.

3.6 Domaine de surveillance

L'autorité de surveillance cantonale change de nom et devient l'autorité cantonale de protection des données. Comme son rôle premier est de conseiller, de guider et de former, non pas de contrôler et de sanctionner, son nom doit le refléter. L'objectif est d'empêcher le mauvais usage de données personnelles plutôt que de sanctionner les abus.

Par égard envers l'autonomie communale, chaque commune et autre collectivité de droit communal dispose aujourd'hui, pour son domaine, de sa propre autorité de surveillance qui assume le rôle d'autorité de protection des données. La présente révision doit offrir un cadre où les tâches des communes sont allégées. Toutes les autorités communales de protection des données ne peuvent assurer la même qualité et la même disponibilité. Généralement, le mandat est assumé par l'organe de vérification des comptes ou la commission de gestion, qui ne disposent pas nécessairement des connaissances spécialisées requises, soit parce qu'ils n'ont pas de savoir-faire en la matière soit parce que les cas ne se présentent pas assez fréquemment. La protection des données soulève des questions complexes et leur traitement devient toujours plus exigeant. L'évolution des technologies notamment (comme l'utilisation croissante des services en nuage) requiert aussi un vaste bagage de connaissances qu'il faut tenir à jour dans le domaine de la sécurité de l'information. La situation est telle qu'aujourd'hui déjà le Bureau cantonal pour la surveillance de la protection des données reçoit régulièrement des demandes de la part des autorités communales, qu'il doit pour des raisons de compétence renvoyer aux autorités communales de protection des données. En outre, le fait que chaque autorité communale de protection des données procède aux mêmes analyses juridiques et veille au respect des prescriptions applicables en la matière n'est guère efficace. Bien souvent, ni le personnel de l'autorité ni la population ne savent qu'il existe dans leur commune un organisme compétent pour les affaires relevant de la protection des données.

Un nouveau modèle a été développé conjointement par l'autorité cantonale de protection des données, l'Office des affaires communales et de l'organisation du territoire (OACOT), l'Association des communes bernoises (ACB) et le Directoire des préfectures, avec le concours de plusieurs communes de différentes tailles. Sur la base de ce modèle, les tâches jusque-là attribuées aux autorités communales de protection des données doivent être transférées à l'autorité cantonale. Font exception les quatre communes les plus peuplées du canton (Biel/Bienne, Berne, Köniz et Thoune). Le travail de l'autorité cantonale de protection des données se concentrera sur les prestations de conseil ainsi que sur l'accompagnement et sur la formation des autorités communales. Le niveau de protection des données dans les communes doit s'en trouver relevé et les ressources allouées permettront de gagner en efficience. La centralisation sera financée par la compensation des charges; à noter que des économies sensibles sont plausibles compte tenu du potentiel de synergies.

3.7 Systématique du droit

Le contenu de la loi est revu dans son ensemble, ce qui ne va pas sans s'accompagner d'une modification de la systématique. Différents chapitres et articles sont ainsi déplacés.

La systématique devant garantir la lisibilité de l'acte, il convient de subdiviser les chapitres concernant le traitement de données personnelles et l'autorité de protection des données en plusieurs sections. Comme dans la législation fédérale, un chapitre distinct est consacré aux obligations des autorités et à celles des tiers mandatés. Ce chapitre remplace le chapitre actuel sur les fichiers. Le chapitre sur la procédure et la protection juridique est déplacé plus loin dans l'acte, comme il est d'usage dans la législation bernoise, et sa place est reprise par le chapitre sur les autorités de protection des données. Le tableau ci-après permet de comparer les systématiques.

– LCPD	– P-LCPD
– 1 Dispositions générales	– 1 Dispositions générales
– 2 Traitement de données personnelles	– 2 Traitement de données personnelles
–	– 2.1 Principes – 2.2 Formes particulières de traitement – 2.3 Traitement à des fins ne se rapportant pas à des personnes
– 3 Fichiers	– 3 Obligations des autorités et des tiers mandatés – 3.1 Obligations avant la mise en service – 3.2 Obligation d'inscrire au registre des fichiers et au registre des activités de traitement – 3.3 Obligations d'informer – 3.4 Obligations d'annoncer en cas de violations de la sécurité des données
– 4 Droits de la personne intéressée	– 4 Droits de la personne concernée
– 6 Surveillance	– 5 Autorités de protection des données
–	– 5.1 Autorité cantonale de protection des données – 5.2 Autorité de protection des données de droit communal et des Églises nationales – 5.3 Tâches
– 5 Procédure et protection juridique	– 6 Procédure et protection juridique
–	– 7 Dispositions d'exécution
– 7 Dispositions finales	– 8 Dispositions transitoires et dispositions finales – 8.1 Dispositions transitoires – 8.2 Dispositions finales

3.8 Révision d'autres lois

3.8.1 Révision de lois spéciales

Des modifications indirectes ne sont apportées à d'autres actes législatifs que dans la mesure où la révision de la loi cantonale sur la protection des données fait naître des contradictions, des lacunes ou des incertitudes dans la législation spéciale. Une modification indirecte n'est par ailleurs admise que pour les mêmes types d'actes. En conséquence, la modification d'un décret ou d'une ordonnance fait nécessairement l'objet d'un projet distinct[12].

La loi cantonale sur la protection des données est ce qui s'appelle une loi transversale. Cela signifie que les principes de la protection des données – comme l'exigence d'une base légale, le principe de finalité, le principe de la bonne foi, la proportionnalité, l'exactitude des données ou la sécurité des données – doivent être observés par toutes les autorités auxquelles la loi cantonale sur la protection des données s'applique. Il faut noter que cette loi ne contient toutefois pas de base légale pour un traitement concret de données; c'est la loi spéciale qui fournit une telle base. La base juridique ne répond pas aux mêmes exigences selon le type de données personnelles traitées (voir le commentaire de l'art. 4 P-LCPD). Les lois indiquées ci-après sont modifiées dans le cadre de la révision.

[12] Sur l'ensemble du sujet, voir les Directives sur la technique législative, module 3, ch. 2.2.4.2

3.8.2 Loi du 7 mars 2022 sur l'administration numérique (LAN)[13]

Les dispositions de la loi qui concernent la protection des données, conçues à titre provisoire, sont reprises légèrement modifiées dans la loi cantonale sur la protection des données. Des détails sont fournis au point 7.9.2.

3.8.3 Loi du 12 septembre 1985 sur l'établissement et le séjour des Suissesses et des Suisses (LES)[14] et loi du 9 décembre 2019 portant introduction de la loi fédérale sur l'asile et de la loi fédérale sur les étrangers et l'intégration (Li LFAE)[15]

La loi révisée réunit synthétiquement les prescriptions relatives à la communication de données personnelles, tandis que leur communication par les communes municipales sont désormais réglées au niveau de la législation spéciale (voir le point 7.9.3). Dans le dernier cas, il s'agit de droit matériel de la protection des données, qui n'a pas à être considéré dans l'ordre juridique comme une matière transversale. Sa place dans la loi actuellement en vigueur est tout à fait inhabituelle.

3.8.4 Loi du 20 juin 1995 sur l'organisation du Conseil-exécutif et de l'administration (loi d'organisation, LOCA)[16]

L'autorité cantonale de protection des données est, comme le Contrôle des finances, une autorité de surveillance indépendante sur les plans organisationnel et institutionnel. Dans un souci de leur garantir un statut identique, le titre 2a doit être complété de manière à mentionner l'autorité cantonale de protection des données. Il faut aussi qu'un nouvel article 40b soit créé, sur l'exemple de celui du Contrôle des finances, désignant l'autorité cantonale de protection des données comme étant une unité administrative autonome. De plus, il convient de noter que, sous un angle structurel, l'autorité cantonale de protection des données fait partie de l'administration. Le sujet est abordé plus en détail au point 7.9.4.

3.9 Dispositions écartées

3.9.1 Ordonnance exploratoire

Une ordonnance exploratoire permet d'essayer de nouvelles formes d'action de l'administration. La législation expérimentale sert à évaluer les effets d'une possible nouvelle réglementation et, ainsi, à offrir de meilleures bases à la décision du législateur dans le cadre de la procédure législative ordinaire. À l'occasion d'une consultation préliminaire menée au sein de l'administration, la proposition a été faite d'examiner l'opportunité de la création d'une base légale pour l'édiction d'ordonnances exploratoires dans la loi cantonale sur la protection des données. L'article 44 LOCA constitue à ce sujet une base légale suffisante. L'alinéa 3 prévoit expressément que ces ordonnances peuvent contenir des dispositions dérogeant aux lois cantonales. Les prescriptions du droit fédéral, du droit constitutionnel cantonal et des conventions intercantonales restent néanmoins applicables. Par conséquent, le traitement de données sensibles peut aussi selon

[13] RSB 109.1
[14] RSB 122.11
[15] RSB 122.20
[16] RSB 152.01

les circonstances être réglé dans des ordonnances exploratoires pour autant que soient respectés les principes de délégation prévus à l'article 69, alinéa 4 ConstC. Il faudrait en particulier que la tâche rendant le traitement de données sensibles nécessaire soit réglée dans la loi.

3.9.2 Conseillère ou conseiller à la protection des données

Dans le domaine de la police et de la justice, l'article 32 de la directive (UE) 2016/680 prévoit que les autorités désignent une déléguée ou un délégué à la protection des données dont la tâche est de conseiller l'administration sur les sujets touchant à la protection des données. Il ne faut pas confondre les personnes désignées comme déléguées au sens du droit européen avec les déléguées, délégués, préposées et préposés qui exercent leur fonction aux niveaux fédéral et cantonal, car leur mandat relève d'une activité indépendante de surveillance. Les tâches des déléguées et délégués à la protection des données au sens de la directive (UE) 2016/680 correspondent, dans le canton de Berne, à celles assumées par l'organe de contact interne qui doit être désigné au moins par chaque Direction et par la Chancellerie d'État pour la protection des données conformément à l'article 15 de l'ordonnance du 22 octobre 2008 sur la protection des données (OPD)[17]. Les juristes des offices, le cas échéant, assument également la fonction d'organe de contact pour leur domaine de compétence. Leurs attributions portent sur les activités de surveillance et de conseil ainsi que sur la collaboration avec l'autorité cantonale de protection des données. Ces organes de contact sont l'équivalent des conseillères et conseillers à la protection des données au niveau fédéral (art. 10, al. 4 LPD) et leur désignation sera reprise dans la terminologie cantonale dès l'entrée en vigueur de la révision de l'ordonnance sur la protection des données. Selon l'article 150 de la loi du 10 février 2019 sur la police (LPol)[18], le même rôle est dévolu à la personne chargée de la protection des données. Cette appellation aussi doit être changée, ce qui implique une modification indirecte de la loi sur la police. Dans l'exécution des peines et mesures, la fonction est assumée par la juriste compétente ou le juriste compétent de l'office. L'impulsion de l'autorité cantonale de protection des données doit permettre aux relations entre les organes de conseil de s'intensifier et ainsi au niveau de protection des données, de s'améliorer.

L'imputabilité de la protection des données aux autorités responsables est à l'origine de l'obligation faite aux organes de l'administration de désigner une conseillère ou un conseiller à la protection des données. Selon le principe de l'autonomie organisationnelle du Conseil-exécutif, l'attribution de cette tâche doit être fixée par voie d'ordonnance.

Toutefois, les tribunaux et les autres autorités judiciaires indépendantes, comme le Ministère public, peuvent être dispensés de cette obligation dans l'exercice de leur fonction juridictionnelle. Le législateur renonce donc à arrêter une disposition à cet égard. Pour tout ce qui ne relève pas de la fonction juridictionnelle, la tâche ressortit à la Direction administrative de la magistrature en sa qualité d'organe d'administration autonome commun de la Cour suprême, du Tribunal administratif et du Parquet général.

3.9.3 Disposition relative à la responsabilité

Conformément aux dispositions générales du droit de la responsabilité et de la responsabilité de l'État, la loi cantonale sur la protection des données prévoyait jusqu'à présent qu'un traitement illicite de données conférait un droit à la réparation morale et à des dommages-intérêts (art. 25 LCPD). Il s'agit en l'occurrence d'une norme de la législation spéciale, qui prime en principe les règles générales. Cependant, la disposition ne se distingue pas matériellement des

[17] RSB 152.040.1
[18] RSB 551.1

règles générales régissant la responsabilité de l'État et n'a donc pas de portée spécifique[19]. Selon l'article 100 de la loi sur le personnel (LPers)[20] en particulier, le canton répond en effet du dommage que les tiers mandatés ont causé. Dans un jugement qui traite explicitement la question de la responsabilité pour des dommages causés par des auxiliaires, le Tribunal administratif a conclu que le canton devait se laisser imputer leur comportement même en l'absence de base légale expresse[21]. Par conséquent, il n'y a pas lieu de transposer la disposition dans le nouveau droit. Les dispositions générales de la loi sur le personnel concernant la responsabilité du canton sont applicables par analogie.

4. Forme de l'acte législatif

Le droit à la protection des données est un droit constitutionnel (art. 18 ConstC). Ses traits caractéristiques doivent être réglés dans une loi. En font partie les règles matérielles fondamentales de la protection des données, par exemple les principes régissant le traitement de données personnelles ou les droits des personnes concernées, et les dispositions définissant les cadres organisationnel et institutionnel, comme la procédure applicable pour faire valoir des prétentions ou l'existence des autorités de protection des données et leur légitimité.

Le droit de la protection des données ne constitue cependant de loin pas une base légale pour le traitement de données personnelles qui limiterait les droits fondamentaux. Il s'agit plutôt d'un droit transversal. Par conséquent, il se contente de définir les grandes lignes du traitement de données personnelles de même que les droits des personnes concernées. Les lois spéciales régissent ensuite les particularités de la matière spécifique. Il en est ainsi notamment des droits particuliers concernant la communication de données personnelles ou des obligations particulières de garder le secret. Une fois le cadre donné par la loi, il suffit que le Conseil-exécutif règle les détails et les modalités par voie d'ordonnance.

5. Droit comparé

Le canton de Berne a ouvert la voie dans la mise en œuvre des exigences de la directive (UE) 2016/680 et a respecté le bref délai imparti. Il a en effet édicté, le 4 juillet 2018 déjà, un acte législatif provisoire: l'ordonnance portant introduction de la directive (UE) 2016/680 relative à la protection des données à caractère personnel. D'autres cantons (Appenzell Rhodes-Intérieures, Argovie, Bâle-Campagne, Fribourg, Lucerne, Saint-Gall, Schaffhouse, Schwyz, Zoug et Zurich) ont aussi transposé les bases légales européennes dans leur droit au second semestre 2022. La situation juridique des cantons d'Argovie, de Saint-Gall, de Zurich et de Lucerne est synthétisée ci-après.

5.1 Canton d'Argovie

Le champ d'application de la loi argovienne sur l'information du public, la protection des données et l'archivage (SAR Nr. 150.700) se limite désormais aux personnes physiques, comme le prévoit également le droit supérieur. Une mention explicite a été ajoutée concernant le droit à la suppression des données et l'obligation d'informer des organes publics lors de la collecte de données personnelles. Le canton d'Argovie a également transposé l'instrument de l'analyse d'impact relative à la protection des données personnelles dans son ordre juridique ainsi qu'une

[19] JAB 2008, p. 49, consid. 6.6.2; Schwegler, Ivo (2021). Informations- und Datenschutzrecht, in: Müller, Markus/Feller, Reto (éd.), Kommentar zum bernischen Verwaltungsrecht. Berne: éditions Stämpfli SA, p. 396
[20] RSB 153.01
[21] JAB 2003, p. 241, consid. 6e

obligation étendue s'agissant de la consultation préalable de la déléguée ou du délégué à l'information et à la protection des données et une obligation d'annoncer quand un traitement non autorisé a lieu ou que des données sont perdues et que la situation présente un risque pour la personne concernée. Le statut de la déléguée ou du délégué a été renforcé du fait qu'au terme de son enquête elle ou il peut désormais rendre une décision à l'encontre des autorités.

Certains articles, qui concernaient les projets pilote et les évaluations, ont été abrogés, de même que les dispositions sur le registre des fichiers, tandis que des prescriptions concernant les registres des activités de traitement des autorités pénales ont été édictées dans une loi spéciale.

5.2 Canton de Saint-Gall

Le canton de Saint-Gall aussi a exclu les personnes morales du champ d'application de sa loi sur la protection des données (sGS Nr. 142.1) à l'occasion de sa modification. L'analyse d'impact relative à la protection des données personnelles, la consultation préalable et l'obligation d'annoncer les violations de la sécurité des données ont, quant à elles, trouvé leur place dans la législation. Un registre des fichiers continue d'exister, auquel s'ajoute un registre des activités de traitement, qui est tenu par les autorités de justice et de police. La personne à la tête du service cantonal spécialisé dans la protection des données se voit habilitée à rendre des décisions lorsque, selon toute vraisemblance, l'autorité rejettera sa recommandation ou ne s'y conformera pas. De plus, la période de fonction est fixée à quatre ans et la personne élue est compétente pour engager des collaboratrices et des collaborateurs.

5.3 Canton de Zurich

Dans la loi sur l'information et la protection des données (LS Nr. 170.4), le législateur a renoncé à limiter le champ d'application aux personnes physiques. Les modifications portent sur l'analyse d'impact relative à la protection des données personnelles, sur le contrôle préalable ainsi que sur l'obligation d'annoncer les traitements non autorisés ou les pertes de données lorsque les droits fondamentaux de la personne concernée s'en trouvent menacés. Par ailleurs, les devoirs des organes publics responsables en matière d'information sont étendus. L'obligation pour les organes des tribunaux, les autorités pénales et les organes d'exécution judiciaires de désigner une personne compétente afin de les conseiller en matière de protection des données est inscrite dans les lois spéciales. Les tâches de cette personne comprennent les activités de conseil et de soutien auprès de l'autorité responsable dans les affaires relevant de la protection des données, l'analyse d'impact relative à la protection des données personnelles, la communication et la collaboration avec la déléguée ou le délégué à la protection des données. La déléguée ou le délégué à la protection des données peut par ailleurs rendre une décision en cas de violations des dispositions relatives à la protection des données et, par exemple, exiger la fin d'un traitement.

5.4 Canton de Lucerne

Le législateur lucernois a renoncé à inscrire la protection des personnes morales dans la loi sur la protection des données personnelles de son canton (SL Nr. 38), mais a toutefois prévu plusieurs dispositions à cet égard dans des actes législatifs spéciaux. La loi renforce les obligations faites aux organes publics en matière d'information et d'annonce ainsi que les droits des personnes concernées d'être informées sur les données traitées. Pour certains traitements, les

organes publics soumis à la loi sont tenus de procéder à une analyse d'impact relative à la protection des données personnelles. En outre, les tribunaux, les autorités de poursuite pénale et les autorités d'exécution des peines doivent désigner en leur sein une conseillère ou un conseiller à la protection des données. Le statut et l'indépendance dont jouissent les autorités de protection des données ont constitué un point important de la révision. Conformément au standard européen supérieur, la déléguée ou le délégué à la protection des données a le pouvoir de rendre des décisions. La loi règle également les critères d'éligibilité des candidates et des candidats au poste de déléguée ou de délégué et prévoit que la personne soit désignée par le parlement cantonal pour une période de fonction.

5.5 Résumé

Les cantons intègrent de nouveaux instruments dans leur droit, comme l'analyse d'impact relative à la protection des données personnelles, et élargissent la portée des obligations d'informer conformément aux réformes européennes en matière de protection des données. La densité normative varie fortement d'un canton à l'autre. Ainsi, le canton de Zurich ne définit souvent que les principes, tandis que d'autres cantons, comme celui de Saint-Gall, entrent beaucoup dans le détail, les modalités du contrôle préalable en étant un bon exemple. Quant à la question de savoir si la protection des personnes morales continue d'être garantie par la loi cantonale sur la protection des données, les approches retenues sont très différentes. Dans la mesure où les personnes morales sont exclues du champ d'application, les cantons s'inspirent de la réglementation fédérale et édictent en partie des dispositions de protection spécifiques. Quelques cantons réduisent partiellement la charge administrative qu'implique la protection des données, notamment en supprimant l'obligation de tenir un registre des fichiers. Dans tous les cantons consultés, les déléguées et les délégués à la protection des données ont compétence pour rendre des décisions. Aucun des ordres juridiques cantonaux examinés ne prévoit de principe de partition de la législation relevant de la protection des données, qui distinguerait les dispositions applicables aux autorités pénales et aux autorités d'exécution des peines au sens de la directive (UE) 2016/680 de celles concernant le reste de l'administration.

6. Mise en œuvre, évaluation

Le commentaire de chaque article fournit des explications sur la manière dont les dispositions d'exécution concrétisent les normes de la législation. Pour pouvoir s'assurer que la loi est appliquée efficacement, il s'agit de l'évaluer. L'évaluation prendra la forme d'un rapport, rédigé quatre ans après l'entrée en vigueur de la loi par le Conseil-exécutif à l'intention du Grand Conseil.

7. Commentaire des articles

7.1 Dispositions générales

Titre

Un titre court a été donné à la loi fédérale en allemand (*Datenschutzgesetz*). Ce titre court correspond exactement au titre de la loi cantonale du 19 février 1986. Il existe donc un risque certain de confusion, raison pour laquelle le titre de l'acte législatif cantonal est modifié (loi cantonale sur la protection des données [LCPD]).

Article 1 – But

En plus de mettre en œuvre des engagements internationaux, la loi offre une base concrète aux garanties des droits fondamentaux prévues par la Constitution fédérale et la Constitution bernoise. Il s'agit principalement du droit fixé à l'article 13, alinéa 2 Cst., c'est-à-dire le droit à l'autodétermination en matière d'information, traduit dans la Constitution bernoise par le droit à la protection des données (art. 18 ConstC). Cette dernière lie les autorités et détermine les droits de la personne concernée les plus importants (droit de consultation en tant que partie intégrante du droit d'accès, droit à faire rectifier des données personnelles inexactes, droit à la destruction des données personnelles inadéquates ou inutiles).

À la différence de la loi fédérale sur la protection des données, l'acte cantonal ne s'applique pas aux personnes privées; la protection de la personnalité n'y est donc pas mentionnée. Par conséquent, la loi vise expressément à protéger le droit fondamental à la protection des données des personnes dont les données sont traitées par les autorités.

Contrairement aux prescriptions internationales (et à la législation de la plupart des États européens), les lois suisses sur la protection des données protégeaient jusqu'à récemment les personnes morales et les personnes physiques, ce que reflète l'article 1. La loi qui a été adoptée par la Confédération renonce à présent à inclure les personnes morales dans son champ d'application (art. 1 et 2, al. 1 LPD), mais une série de dispositions réglant le traitement de leurs données personnelles est introduite dans la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[22]. Par ailleurs, une disposition transitoire prévoit que d'éventuelles lacunes juridiques pourront être comblées pendant cinq ans dans la mesure où des dispositions de la législation spéciale seront créées pour le traitement des données personnelles des personnes morales.

Les cantons ne sont pas tenus de limiter eux-mêmes le champ d'application de leurs lois en matière de protection des données aux personnes physiques. Une telle limitation aurait pour conséquence le fait que l'ensemble des bases légales réglant le traitement de données personnelles cesserait d'être applicable aux personnes morales et devrait donc éventuellement être adapté. De plus, il faudrait définir le besoin de protection concernant les données des personnes morales. Il est peu judicieux de limiter le champ d'application de la loi cantonale sur la protection des données aux personnes physiques pour qu'en parallèle l'introduction de dispositions distinctes sur le traitement de données personnelles des personnes morales devienne nécessaire dans plusieurs lois spéciales, ce qui ne serait possible par ailleurs qu'au prix d'une lourde charge de travail. Le droit cantonal ne connaît en effet pas d'acte applicable à l'ensemble des autorités: la loi d'organisation ne concerne pas les communes, la loi sur les communes ne vaut pas pour certaines institutions ecclésiales. Quant aux personnes privées assumant des tâches publiques, il n'existe pas non plus d'acte unique. Ainsi, les dispositions sur la protection des personnes morales se trouveraient introduites dans divers actes législatifs et le risque d'en oublier certains, pourtant essentiels, serait réel. Selon l'article 5 Cst., le droit est la base de l'activité de l'État. La base légale exigée ferait défaut si le canton de Berne n'édictait aucune réglementation dans législation spéciale, qui permettrait aux autorités de traiter des données de personnes morales. L'article 18 ConstC repose sur la même idée et va plus loin: en plus de la nécessité d'une base légale et du principe de la proportionnalité, la Constitution cantonale définit certains droits (rectification de données inexactes, destruction de celles qui sont inadéquates ou inutiles) dont les personnes morales peuvent aussi se prévaloir. L'exactitude des données est un autre principe fixé par les normes constitutionnelles. Si tous ces principes devaient être aussi confirmés et concrétisés pour les personnes morales, on verrait naître une législation parallèle, source de confusion, compliquée à appliquer. Circonscrire le champ d'application aux personnes physiques n'est pas judicieux. D'autres y ont également renoncé, comme le canton de Zurich, le canton de Fribourg ou le canton de Schwyz. Quant aux cantons qui ont limité le

[22] RS 172.010

champ d'application aux personnes physiques (le canton de Lucerne, p. ex.), ils ont introduit des dispositions particulières dans les lois spéciales.

Article 2 – Définitions

La majeure partie des définitions coïncide avec celles de la législation en vigueur, bien que certaines soient adaptées à la teneur de la loi fédérale sur la protection des données conformément aux demandes exprimées lors de la procédure de consultation. Les ajouts et les divergences font l'objet des considérations qui suivent. Un nouveau terme est introduit: le profilage à risque élevé. Par ailleurs, la définition des autorités connaît un changement. Par rapport au droit en vigueur, les données personnelles sensibles (appelées jusqu'à présent «données particulièrement digne de protection» ou «données personnelles particulièrement digne de protection») ne sont plus définies dans un article séparé, mais avec les autres termes. Le droit cantonal reprend ainsi la systématique de la loi fédérale sur la protection des données. Une autre différence par rapport au droit actuel concerne la subdivision de l'article. Les définitions ne sont plus réparties en alinéas, mais en lettres, conformément aux directives de technique législative.

Lettre a

À la différence de la loi fédérale sur la protection des données, les informations relatives à une personne morale identifiée ou identifiable sont aussi considérées comme des données personnelles (voir le commentaire de l'art. 1 P-LCPD).

Lettre b

Par personne concernée, la loi entend toute personne dont les données personnelles sont traitées.

Lettre c

La loi cantonale sur la protection des données continue à désigner une catégorie privilégiée de données personnelles dont le traitement se traduit presque certainement par une atteinte grave portée au droit fondamental à la protection des données et pour laquelle des exigences accrues sont prévues (voir l'art. 4, al. 2 P-LCPD). Le fait que le législateur définisse certaines données personnelles comme étant sensibles est tout à fait contesté. L'élément déterminant doit plutôt résider dans le risque potentiel que présente un traitement pour le droit fondamental à la protection des données. Néanmoins, la catégorisation est conservée dans les directives européennes et par le législateur fédéral. Pour des questions d'application, il est absolument logique de déterminer une catégorie de données sensibles pour lesquelles la loi conçoit des exigences accrues sans que le risque ne doive faire l'objet d'un examen à chaque traitement. La liste est exhaustive, ce qui garantit la sécurité du droit.

La désignation «données personnelles particulièrement dignes de protection» est remplacée en français par «données personnelles sensibles (données sensibles)», formulation retenue au niveau fédéral. La version allemande utilisant la même terminologie que la Confédération, les modifications indirectes qui s'y rapportent se limitent aux dispositions en français.

Chiffre 1

Jusqu'à présent, la loi ne mentionnait pas explicitement les opinions et les activités syndicales parce qu'elles étaient comprises dans les opinions politiques et philosophiques. La présente révision sert à l'harmonisation avec le droit européen et avec les textes de la Confédération de sorte que l'appartenance syndicale est intégrée à la liste des données sensibles. Il devient ainsi clair que l'appartenance à un syndicat est une donnée personnelle sensible. La question n'est pas sujette à interprétation. La notion d'appartenance est délaissée pour que le texte soit plus proche de la loi fédérale sur la protection des données.

Chiffre 2

Le terme d'«origine ethnique» vient remplacer celui d'«appartenance raciale». Il s'agit de faire référence à l'appartenance à un groupe de personnes qui, unies par leur culture, leur histoire, leur langue, leurs us et coutumes et leurs traditions, se sentent former une communauté différente du reste de la population et/ou qui sont perçues comme faisant partie d'un groupe distinct par le reste de la population.

À la différence de la Confédération et du droit actuel, la loi cantonale sur la protection des données n'utilisera plus l'adjectif «racial». Aujourd'hui, on peut déjà remettre en question la notion. Il convient bien moins d'y voir une tentative (indéfendable scientifiquement) de classer les êtres humains en «races» selon des caractéristiques extérieures que d'offrir une protection contre les discriminations[23]. Dans la loi cantonale sur la protection des données, il est possible de renoncer à utiliser ce terme car, contrairement à d'autres domaines juridiques, l'intention n'est pas de rattacher des conséquences juridiques aux comportements de discriminations raciales. À cela s'ajoute également le fait que des autorités n'ont pas besoin de telles données pour remplir les tâches qui leur incombent. Les données sensibles sont plutôt celles sur l'origine ethnique.

L'origine ethnique n'ayant rien de commun avec la santé et la sphère intime, elle continue d'être mentionnée dans un chiffre à part.

Chiffre 3

Dans une volonté d'harmonisation avec la législation fédérale, la loi bernoise mentionne dorénavant les informations sur la santé et la sphère intime comme type de données sensibles au lieu de «la sphère intime de la personne». Le contenu de la disposition reste identique.

Les informations relatives à la santé comprennent toutes les indications qui permettent de tirer des conclusions sur l'état de santé physique ou psychique d'une personne. Sont comprises toutes les données qui, au sens le plus large, correspondent à des résultats médicaux. Il ne s'agit pas simplement des diagnostics médicaux classiques. Les informations figurant sur les factures de la patientèle, de même que les anamnèses médicales, les résultats et les informations sur les thérapies sont des données sensibles, puisqu'elles rendent possibles des conclusions sur l'état de santé d'une patiente ou d'un patient[24].

Le Tribunal fédéral distingue, selon la théorie des trois sphères[25], la sphère intime, la sphère privée et la sphère publique. La sphère intime comprend toutes les informations relatives aux affaires privées de la personne concernée, comme sa vie sexuelle, qui restent en principe soustraites à la connaissance d'autrui sauf si la personne concernée les divulgue.

Chiffre 4

La loi considère pour la première fois les données génétiques comme des données sensibles. Les données génétiques sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN (art. 3, lit. *l* de la loi fédérale du 8 octobre 2014 sur l'analyse génétique humaine [LAGH])[26].

Chiffre 5

Par données biométriques, on entend ici les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'un individu qui permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images du visage ou de l'iris, d'indications sur la motri-

[23] Voir Rudin, Beat (2014). Praxiskommentar zum IDG des Kanton Basel-Stadt. Zurich, Bâle, Genève: Schulthess Médias Juridiques SA, n. 37 ad § 3, n. b. p. 71
[24] Blechta, Gabor P. (2014). Zweck, Geltungsbereich und Begriffe, in: Maurar-Lambrou, Urs/Blechta, Gabor P. (éd.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, Bâle: éditions Helbing Lichtenhahn, n. 33 ad art. 3
[25] ATF 97 II 100 s., consid. 3 = JdT 1972 I 244; ATF 118 IV 45; ATF 119 II 222 ss., consid. 2b
[26] RS 810.12

cité, la démarche ou encore d'un enregistrement 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[27].

Chiffre 6

Les mesures d'aide sociale restent considérées comme des données sensibles. Ces mesures englobent les prestations sociales liées au besoin, aussi bien sur le plan financier que sous la forme d'un recours à des institutions d'encadrement ou de conseil. La notion ne se limite pas aux mesures d'aide sociale ou aux programmes d'action sociale. Elle se définit plus largement et comprend notamment les prestations complémentaires, les montants octroyés au titre de la réduction des primes d'assurance-maladie, l'avance de contributions d'entretien, les allocations de formation ou les prestations de l'aide aux victimes[28].

À la différence de l'acte fédéral, la loi cantonale sur la protection des données désigne expressément les mesures de protection de l'enfant et de l'adulte. Actuellement, seules les mesures d'assistance sont citées comme données sensibles. Il convient toutefois de noter que les mesures de protection de l'enfant et de l'adulte sont déjà conçues aujourd'hui comme telles[29]. Les indications sur les placements à des fins d'assistance comptent notamment au nombre de ces données. L'occasion de la présente révision est saisie par le législateur pour remplacer le terme de «mesures d'assistance» par «mesures de protection de l'enfant et de l'adulte» dans le reste des lois (voir le point 7.9.6).

Contrairement aux mesures d'aide sociale, les mesures de protection de l'enfant et de l'adulte sont souvent ordonnées contre la volonté des personnes concernées. Les deux catégories ont cependant en commun le fait que les personnes concernées dépendent de l'aide de l'État. Il leur est souvent désagréable de recourir à de telles prestations ou de voir ordonner une mesure à leur encontre, ce qui explique pourquoi toute indication à cet égard est considérée comme une donnée sensible.

Chiffre 7

La disposition est calquée sur celle de la Confédération et complétée par la mention des poursuites ou sanctions administratives. Ainsi, en plus des données personnelles sur l'ouverture, le déroulement et l'issue de poursuites et de sanctions des autorités de justice pénale, les données personnelles qui ont trait aux procédures disciplinaires (p. ex. interdiction d'exercer une profession) ainsi que les informations relevant de l'exécution des peines sont considérées comme des données sensibles. Parmi les cas concernés comptent aussi les décisions administratives comme le retrait du permis de conduire, l'interdiction de détenir des animaux ou le séquestre d'animaux.

Lettre d

Jusqu'à présent, la loi cantonale sur la protection des données ne comportait aucune définition s'appliquant aux données sensibles des personnes morales. La définition est reprise de la législation fédérale. Le champ d'application détermine la mesure dans laquelle les personnes morales sont soumises à la loi cantonale sur la protection des données (voir le commentaire de l'art. 3, al. 1, lit. *b* P-LCPD).

Lettre e

La notion de fichier doit être reprise du droit actuel. Les autorités cantonales responsables annoncent leurs fichiers à l'autorité cantonale de protection des données, qui les publie dans un registre (art. 42, al. 2 P-LCPD).

[27] FF 2017, ch. 9.1.3.1, p. 6641
[28] voir Rudin, Beat (2015), in: Baeriswyl, Bruno/Pärli, Kurt (éd.), Datenschutzgesetz (DSG). Berne: éditions Stämpfli SA, note 27 ad article 3
[29] Voir, pour le canton de Bâle-Ville au sujet de la notion de mesures d'aide sociale, Rudin, Beat (2014), *op. cit.*, n. 38 ad § 3

Lettre f

La notion de traitement se distingue sur de nombreux aspects du sens que lui donne la Confédération. La précision du texte fédéral «quels que soient les moyens et procédés utilisés» est ajoutée à la définition cantonale. Des formes de traitement sont aussi reprises de ce texte: l'enregistrement, l'utilisation, l'archivage et l'effacement. La liste des opérations entrant en ligne de compte n'est pas plus exhaustive qu'aujourd'hui; d'autres opérations de traitements sont envisageables (structuration, adaptation, extraction de données, etc.).

L'article 3, chiffre 4 de la directive (UE) 2016/680 règle désormais le «profilage» comme un mode de traitement des données personnelles particulier présentant un risque. Il ne s'agit donc pas d'un type de données personnelles, mais d'un mode de traitement. La notion de «profilage à risque élevé» est définie à la lettre *h*.

La notion de destruction est plus forte que celle d'effacement et implique que les données soient éliminées irréversiblement. Lorsque les données sont sur papier, ce dernier devra être brûlé ou déchiqueté. Lorsqu'elles sont sur un support informatique, la destruction est plus complexe. Les ordres habituels de suppression ou un pur reformatage ne représentent pas une destruction, mais un effacement[30].

Lettre g

La notion de communication prend les contours de la définition retenue par le législateur fédéral. La communication se caractérise non seulement par le fait de rendre accessibles des données, mais aussi de les transmettre. L'énumération des exemples est maintenue afin que la portée de la notion devienne concrète.

La communication de données personnelles est une sous-catégorie de traitement. Par cette opération, les données personnelles sortent du domaine de compétence de l'autorité qui en était jusqu'alors responsable. La communication peut éventuellement impliquer un changement de finalité. La question de savoir si l'accès aux données personnelles est accordé à une autre autorité ou à un tiers de manière intentionnelle ou à la suite d'une négligence n'a aucune importance.

Lettre h

Le profilage correspond à un mode spécial de traitement, constituant un processus dynamique qui est orienté vers une finalité particulière. À l'échelon fédéral, une différence est faite entre deux types de profilage: le profilage et le profilage à risque élevé. Si le premier correspond à la définition de la directive (UE) 2016/680 et du règlement général sur la protection des données, le second est une création des Chambres fédérales. Les débats politiques ont en effet révélé que les profilages ne sont pas tous risqués.

Pour autant que l'exploitation soit le fait d'une autorité, la loi fédérale sur la protection des données ne prévoit à première vue pas d'exigences distinctes pour les deux types de profilage. Tout profilage requiert ainsi nécessairement une base légale au sens formel (art. 34, al. 2, lit. *b* LPD). Par contre, une base légale prévue dans une loi au sens matériel suffit si le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel *et* que la finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée (art. 34, al. 3 LPD). Le canton reconnaît également que tous les profilages ne présentent pas nécessairement un risque élevé pour la personne concernée. Le projet soumis lors de la procédure de consultation comportait une restriction (art. 4, al. 2) s'apparentant à la solution retenue au niveau fédéral: une base légale qualifiée n'était requise que pour les profilages présentant des risques particuliers pour la personne concernée. Il est toutefois plus élégant de ne définir que le profilage à risque élevé, comme le législateur fédéral, et de n'imposer des exigences qualifiées concernant une base inscrite dans la loi que pour ce type de profilage

[30] voir à ce sujet: FF 2017, p. 6641

(voir l'art. 4 P-LCPD). C'est aussi l'option retenue dans le projet du canton de Zurich notamment (voir l'art. 5, al. 4, lit. *c* et l'art. 25, al. 1, lit. *a* du projet de loi zurichois sur l'information et la protection des données [*Gesetz über die Information und den Datenschutz (IDG)*]). Il est ainsi également tenu compte des critiques exprimées lors de la procédure de consultation, selon lesquelles la catégorisation d'un profilage comme présentant un risque élevé n'était pas claire, ni la mesure dans laquelle il se rapportait au profilage à risque élevé au sens retenu par la Confédération. Si un profilage ne correspond pas à la notion telle que définie par la loi cantonale sur la protection des données, les exigences concernant la base juridique s'appliquent, puisque des données personnelles sont traitées, voire des données sensibles (art. 4 P-LCPD). Cette solution ne contredit pas non plus les règles européennes. En effet, ces dernières prévoient pour les données sensibles seulement que le traitement soit indispensable à l'accomplissement d'une tâche publique. Par conséquent, des exigences qualifiées valent dans ces uniques circonstances (art. 10 des directives [UE] 2016/680).

Dans un souci de simplicité et d'intelligibilité, la loi cantonale prévoit une définition différente de celle retenue par la Confédération, tout en conservant l'ensemble des éléments constitutifs d'un profilage mais en incluant également les caractéristiques «essentielles» du «profilage à risque élevé». L'élément déterminant repose sur le fait que l'évaluation automatisée vise à analyser ou prédire les aspects «essentiels» de la personne concernée.

Un profilage à risque élevé existe par exemple lorsque l'autorité établit un profil idéal de candidate ou de candidat pour un poste et qu'elle permet une désignation automatisée de la personne y correspondant le mieux sur la base notamment du curriculum vitae, des certificats, des qualifications et des évaluations disponibles.

La liste des aspects particuliers de la personnalité est reprise de l'acte législatif fédéral (art. 5, al. 1, lit. *f* LPD). L'utilisation du mot «en particulier» indique clairement qu'il ne s'agit pas d'une liste exhaustive.

Lettre i

La notion d'autorité du droit actuel (art. 2, al. 6 LCPD) doit être revue. La teneur qui est en vigueur prête à confusion, étant tout à la fois en partie trop restrictive et trop vaste. Le texte modifié explicite le fait que le terme d'autorités est entendu dans un sens très général et correspond à l'idée large et fonctionnelle que lui attribue la Constitution cantonale.

Selon le cinquième titre de la Constitution cantonale, les organes ou les autorités cantonales sont composés du Grand Conseil, du Conseil-exécutif, de l'administration cantonale ainsi que des tribunaux et, après la réforme de la justice, du Ministère public. En raison des prescriptions européennes, les autorités judiciaires (tribunaux et Ministère public) sont aussi soumises au droit cantonal de la protection des données, bien que le droit de procédure applicable contienne des réglementations spéciales (voir l'art. 3, al. 3 P-LCPD).

Par conséquent, la notion d'autorités ne désigne pas seulement les organes exécutifs suprêmes et l'administration, mais comprend aussi les corps législatifs, qu'il s'agisse du Grand Conseil au niveau cantonal ou des parlements communaux au niveau communal. Dans ce cadre, il convient de noter qu'en plus des dispositions spéciales du droit de la protection des données, il existe aussi souvent des règles régissant le secret de fonction et l'obligation de fournir des renseignements, par exemple s'agissant du droit à l'information (voir le 4e titre de la loi du 4 juin 2013 sur le Grand Conseil [LGC])[31].

L'administration cantonale se compose de l'administration centrale et de l'administration de district ou de l'administration décentralisée (art. 92 à 94 ConstC et art. 20 LOCA). L'administration centrale se compose des Directions, de la Chancellerie d'État, des Secrétariats généraux, des

[31] RSB 151.21

offices et des unités administratives qui leur sont assimilées, des services, etc. Les unités administratives doivent être expressément mentionnées étant donné qu'elles sont responsables de la mise en œuvre de la législation sur la protection des données.

En vertu de la Constitution cantonale, les communes municipales, bourgeoises et mixtes sont des collectivités publiques dotées de la personnalité juridique, tout comme les paroisses. Les sections et les syndicats de communes de droit public sont en principe assimilés aux communes (art. 107, al. 1 à 3 ConstC). De par la loi, d'autres collectivités sont encore soumises au droit communal. Il s'agit des corporations bourgeoises, des paroisses générales, des Églises nationales, des corporations de digues et des conférences régionales (art. 2, al. 1 de la loi du 16 mars 1998 sur les communes [LCo])[32]. Les organes communaux sont désignés à l'article 10 LCo. Les unités administratives communales sont aussi responsables de la mise en œuvre du droit de la protection des données, c'est-à-dire en règle générale les directions municipales, offices ou services selon l'organisation de la commune. Naturellement, la loi cantonale sur la protection des données ne s'applique pas au corps électoral.

C'est à dessein que la mention des collaboratrices et des collaborateurs est laissée de côté. Faire peser une responsabilité sur certains membres du personnel contredit les règles du canton en la matière. La responsabilité de la protection des données incombe aux autorités. Dans les faits, les organes de direction en portent la responsabilité pour ce qui relève de leur domaine de compétences. Ils s'engagent pour la protection des données et la sécurité de l'information, sont organisés en conséquence, édictent les dispositions requises, ordonnent les mesures techniques et organisationnelles nécessaires et choisissent soigneusement leur personnel, l'instruisent et le surveillent.

Les unités administratives du canton comprennent aussi les autres organisations chargées de tâches publiques. Les institutions de droit public comme l'Université de Berne ou les collectivités du canton en sont des exemples. Les organisations privées chargées de tâches publiques ne sont toutefois concernées que dans la mesure où elles assument les tâches qui leur sont confiées. Ainsi, une société anonyme de droit privé active dans la couverture des soins (hôpital) n'est une autorité que lorsqu'elle traite des données personnelles dans l'accomplissement des tâches de droit public qui lui sont déléguées. Il en va de même pour les communes, par exemple comme dans le cas des Transports publics biennois ou de l'entreprise de la ville de Berne Energie Wasser Bern[33].

La loi cantonale sur la protection des données s'applique aussi lorsque les données sont traitées par des organes des Églises nationales et de leurs entités régionales selon la loi du 21 mars 2018 sur les Églises nationales bernoises (loi sur les Églises nationales, LEgN)[34], comme c'est le cas aujourd'hui. Cette fois encore, le corps électoral est exclu du champ d'application.

Lettre k

L'autorité cantonale de surveillance prend le nom d'autorité cantonale de protection des données. Elle assume en principe les tâches accomplies jusqu'alors par les autorités de surveillance de droit communal (voir le commentaire du point 3.6). Les quatre communes les plus peuplées (Biel/Bienne, Berne, Köniz et Thoune) continuent d'avoir leur propre autorité de protection des données, tout comme les Églises nationales. Les dispositions s'appliquent à toutes les autorités de protection des données, sauf mention explicite de la loi, lorsque seule l'autorité cantonale de protection des données est concernée.

Dispositions non reprises:

Le terme d'«autorité responsable» n'est pas retenu dans les notions parce qu'il est défini par le droit matériel et qu'il est trop long pour une définition légale (voir l'art. 11 P-LCPD). Le terme

[32] JAB 2013, consid. 4.3, p. 251
[33] Daum Michel (2020), in: Herzog, Ruth/Daum, Michel (éd.), Kommentar zum Gesetz über die Verwaltungsrechtspflege des Kantons Bern. Berne: éditions Stämpfli SA, n. 19 ad art. 2
[34] RSB 410.11

«sous-traitant» qui se retrouve dans le texte fédéral n'est pas non plus repris car la formulation n'est pas inclusive. La loi cantonale lui préfère la notion de «tiers mandatés».

Article 3 – Champ d'application

Alinéa 1

Lettre a

Comme jusqu'à présent, la loi cantonale sur la protection des données vaut en général pour chaque traitement de données personnelles, indépendamment des moyens ou des procédures utilisés. La lettre *a* régit le traitement des données des personnes physiques.

Lettre b

La loi cantonale sur la protection des données ne régit le traitement des données des personnes morales que dans la mesure pouvant être inférée de la Constitution cantonale. Or il convient de noter que la Constitution va relativement loin. L'énoncé de l'article 18 ConstC, en plus de prévoir les droits de la personne concernée (al. 1), conditionne, par l'alinéa 2, tout traitement de données personnelles à l'existence d'une base légale ainsi qu'à la nécessité et l'adéquation du traitement (= proportionnalité) pour l'accomplissement des tâches (= finalité déterminée). De plus, le constituant oblige les autorités à s'assurer que les données traitées sont exactes et à les protéger contre un emploi abusif (al. 3). Par ailleurs, de l'avis du législateur fédéral, les personnes morales peuvent se prévaloir des droits de personnes concernées même si la loi sur l'organisation du gouvernement et de l'administration ne le prévoit pas explicitement[35].

Cela signifie que les principes fixés à la section 2 LCPD valent de par la Constitution cantonale. Les droits des personnes concernées listés à la section 4 sont également applicables. Des exceptions sont possibles en vertu de la section 3 (obligations des autorités et des tiers mandatés) et de la section 5 (autorité de protection des données). Par conséquent, ces sections sont exclues du champ d'application pour les données personnelles des personnes morales.

Alinéa 2

Comme jusqu'à présent, les dispositions de la loi ne s'appliquent pas aux notes personnelles traitées pour un usage exclusivement personnel. Les notes qui servent à d'autres personnes (supérieures ou supérieurs hiérarchiques, suppléantes ou suppléants, successeuses ou successeurs) ne font pas partie de cette catégorie.

Alinéa 3

À l'heure actuelle déjà, les actes des autorités relevant de l'économie privée n'entrent pas dans le cadre du droit cantonal de la protection des données. Tant que des autorités agissent comme des entreprises du secteur privé, il n'y a aucune raison que les règles de la loi cantonale sur la protection de données leur soient appliquées de ce fait. Il y a donc lieu de reprendre telle quelle la teneur des dispositions du droit en vigueur (art. 4, al. 2, lit. *a* LCPD). L'autorité agit en situation de concurrence économique lorsqu'elle se trouve en compétition avec d'autres actrices et acteurs sur le marché et que, par ses prestations, elle réalise des gains. Cela signifie que les autres parties au contrat doivent être libres de leur choix lors de la conclusion et que leurs droits et obligations ne doivent pas découler d'une décision ou résulter d'un contrat de droit administratif[36]. Toutefois, les nouvelles prescriptions veulent que des règles relevant de la protection des données soient opposables – comme c'est le cas pour les personnes privées, qui sont soumises à la loi fédérale sur la protection des données. Logiquement, de tels traitements de don-

[35] FF 2017, p. 6734
[36] Rudin, Beat (2014), *op. cit.*, n. 13 ad § 2

nées sont régis par la loi fédérale sur la protection des données, ce qui est désormais explicitement mentionné dans la loi cantonale. L'application se fait seulement par analogie, car il n'est pas possible pour le droit cantonal d'étendre les limites de la loi fédérale.

Étant donné que les autorités ne deviennent pas des entités privées, mais agissent seulement en cette qualité, elles sont assujetties à la surveillance cantonale même dans leurs entreprises privées. Le préposé fédéral à la protection des données et à la transparence (PFPDT) ne se considère explicitement compétent que dans la surveillance des organes fédéraux et des personnes privées. Il n'existe pas de domaine libre de toute surveillance[37]. Cette dernière est régie par les dispositions cantonales.

Il convient de noter que la loi cantonale sur la protection des données ne s'applique aux personnes privées que dans la mesure où elles accomplissent des tâches de droit public à elles confiées (art. 2, al. 1, lit. *h*, ch. 2 P-LCPD). La disposition concerne ainsi des autorités constituées en vertu du droit public (art. 2, al. 1, lit. *h*, ch. 1 et 3 P-LCPD).

Alinéa 4

Cet alinéa règle le rapport entre le droit de procédure et le droit de la protection des données. Selon le droit en vigueur, les procédures pendantes en matières civile, pénale et de droit administratif ne peuvent être régies que par les lois procédurales applicables (art. 4, al. 2, lit. *c* LCPD). Ces dernières régissent en particulier le droit d'être entendu, le droit de consulter le dossier et l'obligation de motiver. Or il n'est plus permis, en raison des prescriptions européennes, d'ériger en principe général une exception pour les procédures judiciaires pendantes qui revêtirait une forme aussi absolue. Conformément à l'article 14, paragraphe 1 STE n° 108+, les exceptions admises concernent seulement le principe de la bonne foi, le principe de finalité, le principe de proportionnalité, le principe de l'exactitude des données ainsi que l'obligation d'annoncer les violations de la sécurité des données, l'obligation d'informer et les droits de la personne concernée. Dans le premier cas, il s'agit de principes constitutionnels de l'État de droit, dont le droit cantonal doit tenir compte.

La loi cantonale sur la protection des données est une loi qui porte sur plusieurs branches du droit. Des lois spéciales doivent la compléter ou peuvent y déroger en tant que droit spécial. En ce sens, les lois procédurales, en tant que droit propre à la branche concernée (ou droit matériel), complètent aujourd'hui déjà le droit formel de la protection des données. Par exemple, le droit de la protection des données exige que tout traitement de données personnelles soit prévu par une base légale, que la législation spécifique, c'est-à-dire le droit de procédure applicable, fournit. L'ampleur de la dérogation aux règles cantonales sur la protection des données que permet la loi spéciale est à décider au cas par cas.

Le nouvel alinéa entreprend de définir clairement les limites entre le droit de la protection des données et le droit procédural faisant office de législation spécifique. Il se fonde sur la législation fédérale, selon laquelle seul le droit de procédure applicable régit le traitement des données personnelles et les droits des personnes concernées dans l'ensemble des procédures des autorités judiciaires et des autorités de justice internes à l'administration. Le premier cas concerne toutes les procédures menées auprès des tribunaux du canton de Berne, soit les procédures civiles et pénales ainsi que les procédures administratives portées devant les autorités judiciaires, commissions de recours comprises. La formulation s'appuie sur la loi sur l'organisation des autorités judiciaires et du Ministère public (LOJM)[38]. Le Ministère public aussi doit être mentionné. Pour les procédures administratives, il suffit que l'exception vaille également pour les autorités de justice internes à l'administration. Ces autorités regroupent aussi bien les organes de recours internes à l'administration que les organes internes pouvant être actionnés,

[37] Rudin, Beat (2014), *op. cit.*, n. 17 ad § 2
[38] RSB 161.1

au sens des articles 60 à 73 et 88 de la loi du 23 mai 1989 sur la procédure et la juridiction administratives (LPJA)[39] .

Il convient de noter que les éventuelles dispositions spéciales qui se trouveraient ailleurs que dans les lois procédurales concernées sont comprises dans la notion de droit procédural applicable. Il s'agit notamment de la loi du 1er février 2012 sur la protection de l'enfant et de l'adulte (LPEA)[40] ou de la loi sur le Grand Conseil. L'article 23 LPJA porte sur la consultation des dossiers, comme l'article 53 LPEA, et la loi sur le Grand Conseil a même un titre distinct sur le droit à l'information, le secret de fonction et l'obligation de fournir des renseignements. Les prescriptions procédurales en question garantissent également la sauvegarde des droits fondamentaux de toutes les personnes impliquées, offrant ainsi une protection équivalente à celle de la législation sur la protection des données. Si la loi cantonale sur la protection des données s'appliquait dans ce domaine, on serait confronté à un risque de conflits de normes et de contradictions, qui pourrait perturber la bonne application des règles de procédure.

Le traitement de données personnelles et les droits de la personne concernée sont régis par les prescriptions procédurales applicables devant les autorités mentionnées, notamment par les dispositions du code de procédure civile du 19 décembre 2008 (CPC)[41], du code de procédure pénale suisse du 5 octobre 2007 (code de procédure pénale, CPP)[42] et de la loi sur la procédure et la juridiction administratives. Cela signifie que les droits de la personne concernée (section 4 P-LCPD) sont suspendus durant la procédure et que, par exemple, l'article 53 CPC, les articles 107 et 108 CPP et l'article 23 LPJA s'appliquent concernant les droits d'information. Le droit de procédure applicable régit le traitement des données personnelles, qu'il s'agisse du traitement de données effectué par le tribunal vis-à-vis des participantes ou participants à la procédure ou de celui effectué par les ceux-ci vis-à-vis d'autres participantes ou participants à la procédure. Cela vaut en particulier pour les droits des parties de prendre connaissance des données personnelles intégrées à la procédure et d'en rectifier certaines si nécessaire, de même que pour le traitement de données dans les procédures judiciaires en général. Cela signifie notamment que les différents moyens de recours prévus par la loi cantonale sur la protection des données ne s'appliquent ni au traitement de données effectué par le tribunal dans la procédure, ni à celui effectué par les autres participantes ou participants à la procédure. À titre d'exemple, les participantes ou participants à la procédure ne peuvent pas faire valoir de droit d'accès au sens de la loi cantonale sur la protection des données afin de consulter le dossier au tribunal ou d'obtenir des preuves d'autres participantes ou participants à la procédure. En d'autres termes, il n'est pas possible de s'appuyer sur la loi cantonale sur la protection des données pour entreprendre vis-à-vis du tribunal ou entre participantes ou participants à la procédure des actions relevant de la procédure qui seraient soit exclues selon le droit de procédure en question, soit régies par des règles et des principes bien précis.

Il convient d'abandonner la notion de procédure pendante car elle pose des problèmes de délimitation. En effet, il n'est question de litispendance que dans la procédure civile (art. 62 CPC) et en matière de juridiction administrative (art. 16 LPJA). Ce qui compte, c'est qu'une procédure soit régie par des prescriptions procédurales. Le critère de délimitation essentiel est l'existence ou non d'un lien immédiat avec une procédure. Un tel lien existe lorsque le traitement de données personnelles en question est susceptible d'avoir des effets concrets sur cette procédure ou sur son issue, ou sur les droits procéduraux des parties[43]. Une importance particulière doit être accordée aux procédures d'investigation de la police: le code de procédure pénale réglemente la procédure préliminaire, qui se compose de la procédure d'investigation de la police et de l'instruction conduite par le Ministère public (art. 299, al. 1 CPP). Cette procédure préliminaire est à distinguer de l'activité d'enquête préliminaire de la police durant laquelle il n'existe

[39] RSB 155.21
[40] RSB 213.316
[41] RS 272
[42] RS 312.0
[43] Voir FF 17.059, ch. 9.1.2, p. 6633

qu'un vague soupçon. Cette dernière n'est pas régie par le code de procédure pénale[44]. Ainsi, la loi cantonale sur la protection des données fait foi pour la procédure d'enquête policière préliminaire, pour autant que la loi sur la police n'en dispose pas autrement (art. 141, al. 1 LPol).

La notion de personnes concernées comprend aussi les personnes qui ne relèvent pas des catégories visées à l'article 104 CPP (parties) et à l'article 105 CPP (autres participantes et participants à la procédure), mais qui pourtant disposent d'un droit à l'information (p. ex. les tiers en cas de mesures de surveillance secrètes en vertu de l'art. 279 CPP).

La loi cantonale sur la protection des données continue de s'appliquer lorsque la procédure est close (art. 3, al. 1, lit. *b* de la loi du 11 juin 2009 portant introduction du code de procédure civile, du code de procédure pénale et de la loi sur la procédure pénale applicable aux mineurs [LiCPM][45]). Il en va de même pour les procédures de justice administrative même si l'article 23 LPJA ne le prévoit pas expressément. Par conséquent, l'autorité qui statue ne peut communiquer sa décision à une autre autorité que s'il existe à cet effet une base légale suffisante soit dans le droit de procédure applicable (p. ex. art. 75, al. 1 CPP, ordonnance fédérale du 10 novembre 2004 réglant la communication des décisions pénales prises par les autorités cantonales[46]) soit dans un acte législatif spécial distinct.

Il découle de l'alinéa 4 que le droit cantonal en matière de protection des données est applicable aux traitements de données – notamment relatives au personnel – effectués par les services administratifs de tribunaux et d'autorités. Les tribunaux sont aussi tenus de garantir la sécurité des données dans l'archivage des preuves et des jugements.

Les dispositions de la loi cantonale sur la protection des données continuent de valoir pour la procédure administrative (procédure préalable au prononcé d'une décision). Les autorités administratives n'ont donc pas besoin d'être mentionnées. Selon la lettre *c*, l'exclusion du champ d'application ne concerne que les procédures devant les autorités de justice administrative internes à l'administration.

7.2 Traitement de données personnelles

Article 4 – Base juridique

Cet article prescrit quelle base juridique est nécessaire pour le traitement de chaque type de données personnelles, ce qui explique le nouveau titre de la disposition.

Tout traitement de données personnelles entrepris par une autorité constitue une atteinte aux droits fondamentaux de la personne concernée. Comme expression du principe constitutionnel de la légalité (art. 5, al. 1 et art. 36, al. 1 Cst., art. 28 ConstC), le traitement de données personnelles requiert également une base légale. Dans le canton de Berne, les bases légales peuvent prendre forme dans des lois, des décrets et des ordonnances. Au niveau communal, ce sont des règlements et des ordonnances en principe. Toute restriction grave doit être prévue par la loi elle-même. Les lois (ou, pour l'équivalent communal, les règlements en principe) sont des normes générales et abstraites édictées selon une procédure législative particulière, alors que les décrets et les ordonnances sont des actes législatifs de niveau inférieur. Dans la loi cantonale sur la protection des données, la terminologie a été jusqu'à présent utilisée de manière incohérente et parfois même fausse. Désormais, la notion de «loi» recouvre toutes les normes générales et abstraites qui ont été adoptées à la suite d'une procédure législative particulière. Au niveau cantonal, il s'agit de normes générales et abstraites qui ont été adoptées par le parlement et qui sont soumises au référendum facultatif (art. 69, al. 4 en relation avec l'art. 62, al. 1,

[44] Rapport du Conseil-exécutif concernant la loi sur la police (2017), commentaire de l'article 72, p. 40
[45] RSB 271.1
[46] RS 312.3

lit. *a* ConstC). Les communes peuvent aussi complètement déléguer cette compétence au parlement[47]. Il faut tenir compte du fait que le traitement de données sensibles et la pratique du profilage à risque élevé exigent une base légale prévue dans une loi ou un règlement (voir l'al. 2).

La base légale peut être directe ou indirecte. La base légale directe règle explicitement le traitement de données: elle oblige ou habilite l'autorité à traiter certaines données personnelles[48]. L'article 39, alinéa 3 de la loi du 3 décembre 2020 sur les prestations particulières d'encouragement et de protection destinées aux enfants (LPEP)[49], par exemple, prévoit que les informations sur les données fiscales peuvent être demandées par le service compétent de la Direction de l'intérieur et de la justice aux autorités fiscales.

La base légale indirecte, quant à elle, attribue à l'autorité une tâche qui peut être remplie seulement par le traitement de données personnelles[50]. L'article 144, alinéa 1 LPol en est un exemple: la Police cantonale peut, au cas par cas, communiquer des données personnelles à des autorités, dans la mesure où cela est nécessaire à l'accomplissement, par elle-même ou par l'autorité destinataire, de tâches au sens de la loi sur la police.

Il n'est pas toujours aisé de faire la différence entre une base légale directe ou indirecte. Moins le traitement est défini de manière restrictive dans la base légale, plus grand est le pouvoir d'appréciation de l'autorité. Dans l'application du droit, cette dernière doit alors veiller d'autant plus au respect du principe de proportionnalité.

Alinéa 1

L'alinéa 1 fixe les conditions du traitement des données personnelles. Contrairement au droit en vigueur, dans un souci d'augmenter la lisibilité de l'acte, le législateur a séparé les bases légales directe et indirecte en deux lettres distinctes.

Selon la lettre *a*, il n'est possible de traiter des données personnelles que lorsque la législation l'autorise (base légale directe). L'autorisation n'a pas besoin d'être «expresse», comme le prévoit le droit actuel. Il doit néanmoins être au moins possible de déduire des bases légales l'autorité qui traite les données, la finalité du traitement et les catégories de données personnelles concernées. Par contre, il n'est pas nécessaire que la base légale mentionne l'ensemble des traitements de données.

La base légale indirecte telle que décrite à la lettre *b* correspond en substance au droit actuel. La disposition prévoit qu'une autorité peut procéder au traitement des données personnelles s'il sert à l'accomplissement d'une tâche légale (base légale indirecte).

Alinéa 2

Des conditions supplémentaires continuent de s'appliquer dans les cas où une autorité traite des données sensibles puisque, selon la conception que s'en fait le législateur, ce type de traitement constitue une atteinte grave aux droits fondamentaux. Les mêmes exigences sont aussi prévues pour les profilages à risque élevé (voir le commentaire de l'art. 2, lit. *h* P-LCPD). Si l'autorité n'évalue pas de données personnelles aux fins d'analyse ou de prédiction des caractéristiques essentielles d'une personne physique, il n'en reste pas moins qu'elle traite des données personnelles et qu'elle a besoin à cet effet d'une base légale directe ou indirecte au sens de l'alinéa 1. L'autorité doit apprécier la situation au cas par cas.

Au-delà des exigences de l'alinéa 1, une autorité ne peut traiter des données sensibles ou procéder à un profilage à risque élevé que s'il existe une base dans la loi. La loi peut se limiter à régler les principes; il faut donc pouvoir en inférer l'autorité et la finalité du traitement ou du profilage à risque élevé, de même que les catégories particulières de données. Il n'est toutefois

[47] Wichtermann, Jürg (1999), in: Kommentar zum Gemeindegesetz des Kantons Bern. Berne: éditions Stämpfli, remarque sur la n. 12 ad art. 50 à 60
[48] Rudin, Beat (2014), *op. cit.*, n. 16 ad § 9
[49] RSB 213.319
[50] Rudin, Beat (2014), *op. cit.*, n. 17 ad § 9

pas nécessaire que la disposition de la loi énonce séparément chacune des finalités ou tous les traitements de données. Si tel était le cas, la densité normative serait énorme. D'autres droits fondamentaux peuvent par exemple être restreints sans qu'une loi ne fournisse obligatoirement une réglementation détaillée (voir l'art. 28, al. 1 ConstC). Les catégories de données personnelles traitées peuvent en principe déjà être déduites de la finalité du traitement sans qu'il ne faille de réglementation distincte. Dans les cas où une telle déduction n'est pas possible, les catégories doivent être fixées par voie d'ordonnance, ce qui requiert une norme de délégation dans la loi. D'autres spécificités concernant le traitement de données peuvent être précisées dans une ordonnance. Plus le risque pour la personne concernée est élevé, plus le sont les exigences de concrétisation dans l'ordonnance.

Il convient aussi de transposer le cas où le traitement résulte d'une disposition indirecte de la loi (lit. *b*). Cela veut dire qu'une autorité ne peut remplir la tâche que lui confère la loi qu'en traitant des données sensibles ou qu'en procédant à un profilage présentant un risque élevé. L'accomplissement des tâches doit être «indispensable». Ce terme est repris de la loi fédérale (voir la teneur de l'art. 34, al. 3, lit. *a* LPD). Il n'y a pas de différence sur le fond avec la terminologie utilisée précédemment (l'accomplissement des tâches l'exige impérativement). La Confédération requiert en outre dans ces cas que la finalité du traitement soit exempte de tout risque particulier pour les droits fondamentaux de la personne concernée. En ce sens, la disposition est moins stricte que l'article 34, alinéa 3 LPD. Les personnes concernées doivent être capables de déterminer les données sensibles traitées par l'autorité et la finalité du traitement ou du profilage en se fondant sur les normes instaurant les tâches et les prescriptions de la loi en matière de compétence. Ainsi, ces normes doivent être formulées de manière suffisamment précise. Lorsque les personnes n'ont pas à s'attendre à de tels traitements, une base doit être inscrite dans la loi (lit. *a*). Les cas dont il faut en particulier tenir compte sont ceux qui sortent d'un domaine de tâches particulier au sens où la finalité s'en trouve ainsi changée. Il s'agit par exemple des fois où une autorité communique systématiquement des données sensibles à une autorité ayant un champ d'activité différent (procédures d'appel). Cela correspond au droit actuel, à la différence près que les profilages présentant un risque élevé sont désormais aussi concernés.

Le fait qu'une base de rang inférieur (décret ou ordonnance) suffit lorsqu'une personne concernée consent expressément à un ou plusieurs traitements de données déterminés (lit. *c*) doit également être repris. L'ampleur et le but des traitements doivent être suffisamment définis. C'est à cette seule condition que consentir à plusieurs traitements identiques ou différents devient possible. Le but peut également rendre plusieurs traitements nécessaires. La personne concernée doit toutefois être en mesure d'évaluer les risques. Toute déclaration générale de consentement ou tout blanc-seing sont exclus. Dans un but d'harmonisation avec le droit fédéral, il ne suffit plus que la personne concernée ait donné son accord exprès pour qu'il soit renoncé à une base légale, mais il faut aussi qu'elle ait rendu les données accessibles à chacune et à chacun et ne se soit pas opposée formellement au traitement. Contrairement à ce que prévoit la Confédération, la phrase introductive (avec l'expression «condition supplémentaire») précise qu'en plus du consentement il faut une base juridique, mais qui n'a pas à figurer dans une loi formelle.

Il n'y a pas lieu de reprendre dans le droit cantonal l'obligation pour les traitements de données personnelles de reposer sur une disposition de loi lorsqu'ils sont susceptibles de porter gravement atteinte aux droits fondamentaux (art. 34, al. 2, lit. *c* LPD). Cette exigence découle déjà des Constitutions fédérale et cantonale (art. 36, al. 1 Cst. et art. 28, al. 1 ConstC).

La réserve générale qui existait jusqu'à présent au sujet du secret de fonction ou d'autres obligations particulières de garder le secret (art. 5, al. 5 LCPD) devient caduque. Lorsqu'une autorité est habilitée par la loi à communiquer les données selon l'article 14, alinéas 1 et 2, ni le secret de fonction au sens de l'article 58 LPers ni celui au sens de l'article 320 CP ne constituent un obstacle à la communication des données (voir l'art. 58, al. 5 LPers et l'art. 14 CP).

Les autres obligations particulières de garder le secret que la législation spéciale prévoit (p. ex. secret en matière d'aide sociale), y compris le secret professionnel (p. ex. secret médical) sont dorénavant abordées dans les dispositions qui les concernent, par exemple pour la communication des données.

Article 5 – Traitement en cas de situation de danger particulière

Alinéa 1

En dérogation à l'article 4, le traitement de données personnelles, données sensibles incluses, est aussi admissible lorsqu'il est rendu nécessaire par une situation de danger particulière. 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 règlement général sur la protection des données. En vertu de cette disposition, les organes peuvent traiter des données personnelles si le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et s'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable. L'article 5 inscrit dans la loi une base susceptible d'être invoquée lorsqu'une telle situation se présente. En vertu de l'article 12, alinéa 1 ConstC, l'intégrité psychique est mentionnée en plus de l'intégrité physique.

Même les obligations légales de garder le secret ne font pas le poids face à une telle nécessité. Les intérêts en jeu justifient que ces obligations soient violées.

S'agissant de l'exigence d'une base légale, il est renoncé à inscrire dans le droit cantonal la dérogation que constitue l'autorisation au cas par cas par le Conseil-exécutif (voir l'art. 34, al. 4, lit. *a* LPD). Le fait que le pouvoir exécutif puisse, s'il estime opportun, autoriser le traitement dans un cas précis sans base légale à cet effet n'est guère compatible avec le principe de la légalité.

Articles 6 et 7 – Finalité et proportionnalité

Ces articles ancrent dans la loi les autres principes de l'État de droit et correspondent sur le fond à ce que prévoit le droit actuel (art. 5, al. 3 à 5 LCPD).

Néanmoins, le titre de la disposition laisse directement entendre que la finalité est l'une des composantes de la proportionnalité. Comme jusqu'à présent, le but du traitement de données doit être défini (art. 6, al. 1 P-LCPD). Il ressort des bases légales applicables à l'accomplissement des tâches.

Les données personnelles ne doivent être traitées que dans le but en vue duquel elles avaient été recueillies à l'origine. Un traitement qui poursuivrait une autre finalité est toutefois possible dans les conditions que prévoit explicitement la loi. C'est le cas si une base juridique au sens de l'article 4 P-LCPD ou un consentement exprès pour un ou plusieurs traitements déterminés le permettent. Un renvoi à la loi du 10 mars 2020 sur les fichiers centralisés de données personnelles (LFDP[51]) s'impose. Cette loi règle lesquelles des autorités peuvent accéder à des données personnelles dans le cadre d'une procédure d'appel.

Les traitements visant une autre finalité sont aussi admis lorsque la personne concernée a consenti à un ou plusieurs traitements déterminés.

La conservation de données personnelles est aussi compatible avec la finalité première dans la phase semi-active, pendant laquelle ces données ne sont plus utilisées en permanence pour l'accomplissement des tâches et dans la phase inactive de l'archivage.

Le principe de la bonne foi, établi à l'article 6, alinéa 2, commande un rapport reposant sur la loyauté et la confiance entre les autorités et les personnes privées. Par conséquent, la commu-

[51] RSB 152.05

nication de données personnelles par les autorités ne peut avoir lieu que si la personne concernée doit s'y attendre, sous réserve de dispositions contraires dans la loi cantonale sur la protection des données. À la différence de la teneur en vigueur, l'alinéa 2 est formulé de façon positive.

Selon l'article 7, le traitement de données personnelles doit être proportionné au but poursuivi (actuel art. 5, al. 3 LCPD). Autrement dit, le traitement de données personnelles doit être approprié et nécessaire pour que le but visé soit atteint ou pour l'accomplissement d'une tâche légale; il doit être acceptable pour la personne concernée. La teneur de la disposition doit être adaptée en conséquence. Il est indispensable que le but du traitement des données soit défini (art. 6 P-LCPD).

Article 8 – Exactitude et exhaustivité

Cette disposition correspond à l'actuel article 7 LCPD. Il est dans l'intérêt aussi bien des personnes physiques que des autorités que les données personnelles traitées soient exactes et complètes. La qualité des données sera cependant toujours relative. Il est donc nécessaire de prévoir une procédure de correction telle qu'elle existe (art. 31 P-LCPD). La présente disposition, qui est générale, oblige l'autorité qui traite des données, dans la mesure où l'on peut raisonnablement le lui demander, à s'assurer que les données soient correctes et complètes. Plus les recueils de données sont anciens, moins l'application du principe sera stricte.

Article 9 – Protection des données dès la conception et par défaut

Cet article instaure l'obligation de respecter les dispositions relevant de la protection des données dès la conception et par défaut. La disposition met en œuvre les exigences de l'article 10, chiffre 3 STE n° 108+ et de l'article 20 de la directive (UE) 2016/680; elle correspond à l'article 7 LPD.

Alinéa 1

L'alinéa 1 inscrit dans la loi l'obligation de mettre en œuvre le principe de la technologie au service de la protection des données (*privacy by design*). En conséquence, des mesures techniques et organisationnelles doivent rendre toute violation des dispositions de protection des données impossible ou à tout le moins en réduire la probabilité. Ce principe doit être appliqué dès la conception du traitement.

Les dispositions relevant de la protection des données comprennent toutes les prescriptions garantissant la protection des données à caractère personnel dans le cadre d'un traitement concret, en particulier les principes de traitement, les prescriptions valables en matière de sous-traitance, les règles sur la communication de données personnelles à l'étranger, le droit d'accès, etc. Certains aspects ne sont pas inclus: l'obligation d'annoncer les fichiers à l'autorité de protection des données ou l'obligation d'établir une analyse d'impact relative à la protection des données personnelles et celle de procéder à un contrôle préalable.

Chacune et chacun détermine les mesures organisationnelles et techniques nécessaires qu'il convient de prendre. Dans un premier temps, il y a lieu de définir tous les facteurs essentiels du traitement qui pèsent sur la protection des données. Dans un deuxième temps, il faut s'assurer que le traitement des données se déroule comme prévu et que toutes les prescriptions en matière de protection des données seront respectées. Plusieurs moyens s'y prêtent, en particulier l'édiction d'instructions, l'utilisation du chiffrement, l'automatisation des suppressions, la réglementation des compétences, la conception de règles sur la durée de conservation. Dans un troisième temps, il reste à mettre en œuvre les mesures définies[52].

[52] Voir Rosenthal, David (2020). La nouvelle loi sur la protection des données, in: Jusletter du 16 novembre 2020, n. 44

Alinéa 2

L'alinéa 2 précise les exigences auxquelles doivent satisfaire les mesures visées à l'alinéa 1. Ces mesures doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue ainsi que du degré de probabilité et de gravité du risque que le traitement des données en question présente pour les personnes concernées. L'état de la technique est déterminant pour ce qui est du support de l'information et les mesures à prendre (p. ex. concernant des restrictions d'accès). Le canton édictera une nouvelle loi sur la sécurité de l'information et la cybersécurité (LSIC)[53] et une ordonnance d'application, qui règlent et abordent la thématique de la sécurité de l'information comprenant la protection des données. Conformément à l'article 1 P-LCPD, qui définit le but de la loi, elle vise à protéger le droit fondamental à la protection des données. Dans les dispositions suivantes, la loi évoque plusieurs fois le «risque pour la personne concernée» sans mentionner explicitement le droit fondamental à la protection des données. Toutefois, cette terminologie se rapporte à l'article définissant le but et, ainsi, à ce droit fondamental.

La norme matérialise l'approche fondée sur les risques. Il faut établir un rapport entre le risque pour les personnes concernées induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé pour les personnes concernées, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront fortes[54].

Alinéa 3

Cet alinéa introduit l'obligation de garantir, par des 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. Il concrétise ainsi le principe de *privacy by default*. Ce principe joue un rôle mineur dans les traitements effectué par des autorités, car ils reposent rarement sur le consentement de la personne concernée. Il convient toutefois de fixer ici le principe selon lequel les paramètres par défaut doivent être le moins intrusifs (service, logiciel ou appareil) lorsqu'une autorité prévoit plusieurs options pour le traitement des données personnelles et que les utilisatrices et les utilisateurs sont libres de choisir les réglages.

La garantie de limiter le traitement au minimum requis par la finalité poursuivie est apportée lorsque l'atteinte au droit fondamental à la protection des données de la personne concernée est à son plus bas niveau et non pas par exemple lorsque le volume de données traitées est le plus faible possible.

Il y a lieu de souligner que les réglages respectueux de la protection des données ne s'accompagnent pas d'une interdiction de couplage. L'autorité peut donc décider qu'un traitement particulier ne peut être choisi que si d'autres traitements sont autorisés en même temps. Cette possibilité est au plus limitée par le principe de proportionnalité ou par la liberté de consentement[55].

Article 10 – Sécurité des données

En allemand, le titre de l'article fait l'objet d'un changement terminologique (*Datensicherheit* au lieu de *Datensicherung*).

Alinéa 1

La teneur de l'alinéa 1 est adaptée à la loi fédérale sur la protection des données. Par rapport à l'article précédent (protection des données dès la conception et par défaut), cet article règle la sécurité des données au sens strict. En prenant les mesures techniques et organisationnelles

[53] RSB [à définir]
[54] FF 2017, ch. 9.1.3.1, p. 6649
[55] Voir Rosenthal, David (2020), *op. cit.*, n. 50

prévues, l'autorité veille à la protection des données personnelles s'agissant plus particulièrement de la confidentialité, de la disponibilité et de l'intégrité des informations traitées. Les mesures de prévention pour d'autres violations de la protection des données relèvent en revanche de l'article 9.

Les mesures typiques garantissant une sécurité adéquate des données comprennent les restrictions d'accès, mais aussi les instructions, les formations ou le choix précautionneux du tiers mandaté. Ces mesures ne doivent pas offrir une protection absolue, mais plutôt être raisonnablement proportionnées, d'un point de vue objectif, par rapport au risque de violation de la sécurité des données de la personne concernée. Il appartient à l'autorité de déterminer les mesures qui s'imposent. Des lignes directrices seront édictées par voie d'ordonnance afin que les mesures à prendre soient déterminées (voir l'al. 2) de façon à garantir la flexibilité nécessaire et de manière à tenir compte de la diversité des traitements dont peuvent faire l'objet les données personnelles.

Alinéa 2

Comme indiqué, le canton de Berne édictera une nouvelle législation réglant la sécurité de l'information au-delà de l'aspect de la protection des données personnelles. Il s'agit de la loi sur la sécurité de l'information et la cybersécurité (LSIC) et de son ordonnance. Il est donc renvoyé à cette législation. Les principes de cette loi (2e section) sont applicables par analogie pour la protection des données. Les autorités prennent donc les mesures qui s'imposent selon le besoin de protection constaté pour garantir la confidentialité, la disponibilité, l'intégrité et la traçabilité des données personnelles. Elles s'assurent que les tiers mandatés aussi tiennent compte de ces exigences et mesures. Les degrés de protection et les mesures sont synchronisés dans les dispositions d'exécution y relatives.

Article 11 – Responsabilité

D'après le droit supérieur, la responsabilité du traitement des données doit être clairement attribuée. Cet aspect revêt une importance particulière lorsque plusieurs organes traitent conjointement des données; les responsabilités doivent être transparentes. La disposition actuelle sur la responsabilité ne suffit pas (art. 8 LCPD). Le 7 mars 2022, le Grand Conseil a adopté la loi sur l'administration numérique, comportant une disposition à cet égard qui est en adéquation avec les prescriptions supérieures du droit européen. La réglementation doit être transposée dans la loi cantonale sur la protection des données et les normes provisoires fixées dans la loi sur l'administration numérique doivent être abrogées (voir le point 7.9.2).

Alinéa 1

Contrairement au texte adopté en mars 2022, le fait que l'autorité décide du but et des moyens du traitement ne doit pas être déterminant. Il faut plutôt fixer le principe selon lequel l'organe traitant des données personnelles dans l'accomplissement des tâches qui lui sont dévolues de par la loi ou qui sous-traite l'opération est responsable en même temps de la protection des données. Certes il est vrai que la formulation «qui décide du but et des moyens du traitement des données» est utilisée dans les pays européens ainsi que dans la législation fédérale et qu'elle a été provisoirement introduite dans la législation cantonale, mais il ne faut pas oublier qu'elle a été conçue par les législateurs d'Europe et de Suisse pour inclure les personnes privées et donc reste générique. Dans la loi cantonale sur la protection des données, dont la portée se limite aux traitements effectués par des autorités, il est possible et nécessaire de continuer à lier la responsabilité à l'organe chargé d'une tâche publique et qui répond donc de l'accomplissement de cette dernière et de la constitutionnalité du traitement des données nécessaires à cet effet. La phraséologie reprise du droit actuel permet un positionnement sans équivoque à cet égard, y compris pour ce qui est de la distinction entre l'organe qui s'est vu confié une tâche publique (la ou le destinataire devenant ainsi l'autorité responsable) et la personne

auxiliaire qui agit en tant que tiers mandaté (l'autorité d'origine conservant alors toute responsabilité sur le traitement). La règle mentionne la sécurité des données en plus de la responsabilité en matière de protection des données. Bien qu'elle soit comprise dans les dispositions de la protection des données, une mention permet d'en souligner l'importance.

L'organe qui effectue un traitement de données sur la base d'instructions seulement a qualité de tiers mandaté et non d'autorité, même s'il dispose d'une certaine liberté dans ses choix, concernant par exemple les procédés utilisés, les programmes ou les mesures de sécurité des données.

La question de savoir qui porte la responsabilité se pose par exemple en lien avec l'application de groupe PERSISKA, de l'Office du personnel. Bien que cette application soit utilisée par de nombreux autres offices pour gérer le personnel, les données passent par des réseaux et des serveurs mis à disposition par l'Office d'informatique et d'organisation (OIO) dans le cadre de la fourniture de prestations TIC de base (et donc confiées à des tiers). Les responsabilités doivent alors faire l'objet d'une réglementation (al. 2).

Alinéa 2

Lorsque plusieurs autorités participent au traitement, elles définissent de manière transparente leurs obligations respectives. L'absence de lacune en la matière est ainsi garantie.

Dans l'exemple susmentionné, le principal responsable de la protection des données serait l'Office du personnel en tant qu'office spécialisé. Toutefois, les autorités qui utilisent PERSISKA pour gérer leurs ressources humaines assument elles aussi leur part de responsabilité dans la manière dont elles gèrent les données de leurs collaboratrices et leurs collaborateurs et dont elles accordent les droits d'accès correspondants à leurs responsables du personnel. L'Office du personnel est ainsi tenu d'édicter des dispositions d'utilisation pour définir la responsabilité incombant aux offices utilisateurs en matière de protection des données, par exemple la responsabilité de vérifier régulièrement les droits d'accès. L'OIO, quant à lui, participe aussi au traitement en mettant à disposition les moyens techniques nécessaires liées aux prestations TIC de base. Il règle dans ses directives techniques le niveau de protection et de sécurité des données garanti par ces moyens, de manière que les autorités utilisatrices sachent quelles mesures supplémentaires elles doivent prendre pour atteindre le niveau de protection requis.

Alinéa 3

Par souci de transparence, l'accord qu'ont entre elles des autorités doit être publié. La personne concernée peut ainsi facilement connaître l'autorité qu'elle doit contacter lorsqu'elle veut faire valoir ses droits. Si la personne concernée sait qu'une autorité participe au traitement des données, elle peut aussi s'enquérir auprès d'elle de la répartition des responsabilités.

À l'image du droit fédéral (art. 33 LPD), la loi cantonale sur la protection des données ne contient pas d'obligation expresse de fournir les preuves du respect des dispositions en matière de protection des données que requièrent l'article 12 STE n° 108+ et l'article 4, paragraphe 4 de la directive (UE) 2016/680. Néanmoins, l'autorité de protection des données peut demander de telles preuves (voir l'art. 45, al. 2, lit. *a* P-LCPD).

Article 12 – Traitement par des tiers mandatés

Les articles 22 et 23 de la directive (UE) 2016/680 prescrivent de manière détaillées les conditions dans lesquelles le traitement par un tiers est licite. La directive impose notamment des exigences aux sous-traitantes et sous-traitants, prévoit des exigences de forme et de contenu pour l'adjudication du mandat et définit des prérequis pour le rapport de sous-traitance. La Confédération a repris à son compte le terme de «sous-traitant» et a mis en œuvre les exigences européennes à l'article 9 LPD. La loi fédérale fixe désormais des règles pour la sous-traitance (art. 9, al. 3 LPD). Le canton de Berne a, lui aussi, une disposition réglant le traitement des données par des tiers: l'article 28 LAN, qui s'inspire de la loi fédérale à une exception près. Cette

exception vise à corriger une probable erreur du législateur fédéral: l'article 9, alinéa 2 s'écarte du message et prévoit que le sous-traitant doit uniquement être «en mesure» de garantir la sécurité des données. Ce libellé ne serait pas approprié: ce n'est pas la sécurité potentielle qui est déterminante, mais la sécurité effective. La loi sur l'administration numérique prévoit par conséquent que l'autorité doit s'assurer que le tiers garantit la sécurité des données. La réglementation doit être transposée dans la loi cantonale sur la protection des données et les normes provisoires fixées dans la loi sur l'administration numérique doivent être abrogées (voir le point 7.9.2).

Dans le domaine des TIC, le canton de Berne confie régulièrement le traitement de données à des tiers. Charger un centre de calcul, par exemple la société Bedag qui est en main cantonale, d'exploiter des applications étatiques s'inscrit également dans cette démarche. La Stratégie TIC fait de l'externalisation de ce type de tâches d'exploitation un principe.

Les tiers mandatés traitent des données sur instructions. Les traitements au sein d'une même unité administrative ne constituent par contre pas des cas de traitement sur mandat. Lorsque des données sont stockées en nuage, il s'agit en principe de sous-traitance, qui doit satisfaire aux conditions y afférentes. L'autorité conserve la maîtrise des données, raison pour laquelle elle ne communique pas de données personnelles au sens de la loi sur la protection des données. Toutefois, les dispositions sur la communication de données personnelles à l'étranger sont applicables par analogie lorsque le mandat est traité hors du pays (voir le commentaire sur l'art. 15 P-LCPD).

Alinéa 1

L'alinéa 1 institue un devoir de diligence à la charge de l'autorité dans le but de sauvegarder les droits des personnes concernées en cas de traitement sur mandat. Elle doit s'assurer de manière active que les tiers mandatés respectent la loi dans la même mesure qu'elle (lit. *a*). Cela concerne principalement le respect des principes généraux de protection des données, les règles relatives à la sécurité des données ainsi que celles sur la communication transfrontière. L'autorité doit tout mettre en œuvre pour éviter d'éventuelles violations de la législation sur la protection des données. Elle doit ainsi veiller à choisir soigneusement les tiers à mandater, à leur donner les instructions adéquates et à exercer la surveillance nécessaire. L'idée que le mandat repose sur une loi ou un contrat n'est plus mentionnée. Dans la mesure où la loi autorise à donner à des tiers le mandat de traiter des données personnelles, ces derniers sont régulièrement appelés à remplir une tâche publique. Ils se qualifient alors à leur tour comme des autorités au sens de la loi cantonale sur la protection des données.

Au traitement d'un mandat peuvent s'opposer des obligations tant légales que contractuelles de garder le secret (lit. *b*). Toutes les obligations de garder le secret n'excluent cependant pas l'exécution d'un mandat par des tiers. Font partie des obligations légales de garder le secret: le secret de fonction ainsi que des devoirs spéciaux comme des obligations particulières de se taire et les secrets professionnels. La règle veut qu'une externalisation soit possible même s'il existe un secret de fonction à la condition que l'autorité lie contractuellement les tiers mandatés au devoir de discrétion. En cas d'obligations spéciales de garder le secret et en cas de secrets professionnels, la situation dépend des mesures techniques et organisationnelles que l'autorité prend. Au nombre de ces mesures comptent notamment la pseudonymisation et le chiffrement.

D'un point de vue matériel, la réglementation correspond à ce qui est prévu au niveau fédéral. Contrairement au législateur fédéral qui a retenu la notion d'interdiction, le législateur cantonal opte toutefois pour l'idée d'opposition car un mandat peut être délégué, malgré l'existence d'obligations de garder le secret, dès lors que des mesures organisationnelles ou techniques sont prises.

Le projet soumis à la procédure de consultation comportait un alinéa 2 séparé pour les obligations de garder le secret. Dans cette version du texte, l'autorité devait limiter l'accès aux données que pouvaient avoir les tiers mandatés au strict minimum en présence d'une obligation de garder le secret. Les participantes et participants à la procédure ont jugé la différence avec l'alinéa 1, lettre *b* trop floue et ont critiqué la nature purement déclaratoire de la disposition. Il est vrai que la limitation de l'accès aux données au minimum découle déjà du principe de proportionnalité, raison pour laquelle la disposition est supprimée.

Alinéa 2

La directive (UE) 2016/680 requiert que les tiers mandatés offrent des garanties suffisantes, par la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière que le traitement réponde aux exigences légales. Pour cette raison, les exigences en matière de sécurité des données sont mentionnées explicitement.

Alinéa 3

L'alinéa 3 prévoit que les tiers mandatés ne peuvent pas transmettre le mandat de traitement à d'autres tiers sans le consentement préalable de l'autorité. Le consentement doit être écrit; la forme électronique suffit. Les règles formelles doivent trouver leur expression dans une ordonnance.

Article 13 – Acquisition

Les principes généraux sont suivis de dispositions plus précises au sujet des formes particulières de traitement, comme le fait de collecter ou de communiquer des données personnelles. Les dispositions particulières ne changent rien au fait que le traitement de données personnelles doit toujours respecter les principes le régissant (art. 4 à 12 P-LCPD).

Les principes sous-tendant la collecte de données personnelles qui existent dans le droit actuel (art. 9, al. 1 à 3 LCPD) sont à transposer dans la nouvelle législation. Selon l'article en vigueur, les données personnelles ne sont règle générale pas recueillies auprès d'autres personnes privées que celles concernées. L'expression «règle générale» indique aussi que des exceptions sont possibles. Une exception est admise notamment si le but de l'acquisition des données ne pourrait être atteint sinon.

Les individus peuvent parfois trouver pénible de se voir poser encore et toujours la même question, ce qui explique que la collecte des données personnelles peut se faire aussi au sein de l'administration tant que la loi ne s'y oppose pas.

La personne privée peut alors partir du principe que la collecte de données personnelles n'est possible que dans les cas où il existe un devoir d'information. Lorsqu'il n'y a pas d'obligation de renseigner, l'autorité doit souligner le caractère facultatif de la réponse.

Les obligations d'informer (fixées actuellement à l'art. 9, al. 4 LCPD) seront définies au troisième titre de la loi (obligations des autorités et des tiers mandatés).

Article 14 – Communication

Jusqu'à présent, la loi cantonale sur la protection des données règle séparément la communication aux autorités (art. 10 LCPD) et aux personnes privées (art. 11 LCPD) bien que les dispositions se recoupent pour la plus grande part. Les autres cantons, contrairement à celui de Berne, ne prévoient pas de dispositions séparées. La révision est l'occasion de réunir ces dispositions et d'intégrer les règles de communication par les communes municipales dans des lois spéciales (voir le point 7.9.3). Dans ce dernier cas, il s'agit de droit matériel qui ne doit pas figurer dans le droit sur la protection des données en tant que droit transversal. La présence de cet élément dans la loi en vigueur est inhabituelle.

La communication de données personnelles est une sous-catégorie de traitement. Ainsi, les exigences pour la communication et pour le traitement ne sont fondamentalement pas différentes. Cependant, il convient d'ajouter que les données personnelles peuvent aussi être communiquées à une autre autorité lorsqu'elle est habilitée à les traiter et qu'aucune obligation particulière de garder le secret ne s'y oppose (al. 2).

Alinéa 1

Comme c'est le cas actuellement, la loi exige qu'une communication à une autre autorité ou à une personne privée repose sur une base légale directe ou indirecte. Cette base légale peut correspondre à une norme abstraite à caractère général de n'importe quel niveau législatif, par exemple à des obligations de communication prévues dans une ordonnance d'exécution. L'adverbe «y» met en évidence le fait que la base légale doit se rapporter à la communication. Lorsqu'il s'agit de données sensibles, il convient de tenir compte des exigences accrues auxquelles est soumise la base légale, c'est-à-dire qu'une base doit être inscrite dans la loi ou que la personne concernée a expressément consenti en l'occurrence à la communication ou encore qu'elle a rendu ses données personnelles accessibles à n'importe qui et ne s'est pas opposée expressément au traitement (voir le commentaire de l'art. 4, al. 2 P-LCPD).

Comme mentionné, l'autorité ne peut pas traiter de données personnelles en vertu d'un consentement sans qu'une base juridique ne l'y autorise (voir le commentaire de l'art. 4 P-LCPD). Par contre, elle peut communiquer les données personnelles qu'elle a recueillies conformément au droit si la personne concernée a expressément consenti à un ou plusieurs traitements déterminés ou si elle a rendu ses données personnelles accessibles à tout le monde et ne s'est pas opposée expressément au traitement (lit. *b*). Si l'autorité communique des données personnelles obtenues en toute légalité, elle viole le principe de finalité. En effet, les données personnelles seraient ensuite traitées à une autre fin que celle prévue au moment de leur acquisition. Par conséquent, l'article 6, alinéa 2 P-LCPD prévoit une réserve à cet égard.

Par ailleurs, l'autorité peut communiquer des données personnelles en présence d'une situation particulière de danger (lit. *c*). Dans ce cas non plus, les données personnelles ne sont pas traitées dans le but poursuivi en premier lieu.

Alinéa 2

Comme sous l'ancien droit, il suffit que l'autorité demandant les données personnelles soit habilitée à les traiter. L'autorité procédant à la communication ne doit pas avoir à chercher les bases juridiques qui permettent à l'autorité qui obtient les données personnelles de les traiter. Il appartient donc à l'autorité demandant les données d'exposer les bases juridiques et de prouver dans quelle mesure elles l'habilitent à traiter les données personnelles en question. S'il s'agit de données sensibles, il faut à chaque fois tenir compte des exigences accrues auxquelles doit répondre la base juridique, soit qu'elle figure dans une loi.

Alinéa 3

Des obligations légales de garder le secret peuvent s'opposer à la communication. Il doit s'agir d'obligations inscrites dans la législation, par exemple un secret professionnel ou un secret de fonction particulier (secret médical ou fiscal).

L'autorité doit trancher au cas par cas, en interprétant la législation, si une obligation de garder le secret s'oppose à la communication[56]. Il peut ainsi arriver que des autorités aient le droit de communiquer des données personnelles malgré une obligation particulière de garder le secret.

Voici un exemple: la Direction de la santé, des affaires sociales et de l'intégration charge un partenaire contractuel de mener un programme de dépistage du cancer impliquant, pour les

[56] Voir Ehrensperger, Jennifer (2024), Bekanntgabe von Personendaten. in: Blechta, Gabor P. et Vasella David (éd.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, Bâle: Helbing Lichtenhahn Verlag, n. 62 ad art. 36; notamment au regard de l'ATF 124 III 170

participantes et participants, des analyses répétées. Après un certain temps, le contrat prend fin et le programme se poursuit avec un autre partenaire contractuel. À la lumière des normes légales régissant l'exécution du mandat (c.-à-d. selon la nature de la tâche), la communication des données personnelles du premier partenaire contractuel au second peut s'avérer possible dans le cas d'espèce, car le mandat ne pourrait sinon pas se poursuivre conformément aux dispositions (voir p. ex. l'art. 2 de l'ordonnance sur la garantie de la qualité des programmes de dépistage du cancer du sein réalisé par mammographie [RS 832.102.4]).

Une modification d'ordre rédactionnel est aussi apportée par rapport à la disposition actuelle (art. 14 LCPD): «des intérêts publics majeurs ou des intérêts privés nécessitant une protection particulière» est modifié par «intérêts publics ou privés prépondérants» en vue d'une cohérence au sein de l'acte législatif; il est ici question d'un cas classique de pesée des intérêts. Par conséquent, la communication de données personnelles est toujours refusée, restreinte ou différée si des intérêts publics ou privés prépondérants s'y opposent.

Article 15 – Communication à l'étranger

Selon l'article 15 P-LCPD, l'État destinataire doit protéger le droit fondamental à la protection des données de la personne concernée de manière appropriée. La règle s'applique aussi lors de l'utilisation de services en nuage. Le Conseil-exécutif a envoyé deux variantes en consultation à propos des exceptions. Dans la variante 1, l'autorité ne pouvait déroger à la règle que dans des cas bien définis, alors que la variante 2 prévoyait, en plus, la possibilité d'une exception ne demandant qu'à ce que les conditions de sous-traitance au sens de l'article 12 soient remplies, indépendamment du niveau de protection des données (art. 15, al. 3, lit. *d* PC-LCPD).

Le Conseil-exécutif a décidé qu'un avis de droit devait examiner, en marge de la procédure de consultation, la conformité avec le droit supérieur et la légitimité de la variante 2. L'Office juridique de la DIJ a donc cherché une personne appropriée pour ce faire et a donné le mandat à Madame Astrid Epiney. Madame Epiney est professeure ordinaire de droit international, de droit européen et de droit public suisse à l'université de Fribourg. Elle est aussi responsable des Journées de droit de la protection des données de l'université de Fribourg. Son expertise en matière de protection de données, notamment dans un contexte international, est reconnue et elle publie régulièrement à ce sujet.

L'avis de droit, daté d'octobre 2023 et remis conjointement par Mesdames Astrid Epiney et Nula Frei, a montré que la variante n'était pas admissible au vu du droit international et du droit constitutionnel et n'avait aucune utilité. Le Conseil-exécutif a donc choisi de ne pas garder la variante 2.

Alinéa 1

Les garanties constitutionnelles concernant la restriction des droits fondamentaux doivent être respectées et il n'en va pas autrement lorsque des données personnelles sont communiquées à l'étranger. La règle de base veut ainsi que des données personnelles peuvent être transmises à des États tiers s'ils disposent d'un niveau de protection adéquat (art. 16, al. 1 et 2 LPD, art. 17 STE nº 108+ et art. 36, par. 1 de la directive (UE) 2016/680). Se pose alors la question de la compatibilité de la protection des données assurée par l'État tiers avec les principes constitutionnels définis aux niveaux suisse et cantonal. Ces principes sont les suivants:

- Principe de la légalité (art. 5 et 164 Cst.; art. 18, al. 2, art. 66, al. 2 et art. 69, al. 4 ConstC): Il existe une base légale suffisamment précise et claire pour chaque traitement de données personnelles.
- Principe de la proportionnalité (art. 36, al. 3 Cst.; art. 28, al. 3 ConstC): Les atteintes portées au droit fondamental à la protection des données doivent être adéquates et nécessaires aux buts légaux visés. Elles doivent être supportables pour les personnes concernées.

- Moyens de droit effectifs (art. 13, al. 2 Cst.; art. 18, al. 1 et 3 ConstC): Les personnes concernées doivent pouvoir faire valoir leurs droits (p. ex. droit d'accès, droit à la rectification et à l'effacement des données) en engageant des démarches juridiques effectives et prévues par la loi.
- Garantie de l'accès au juge (art. 29 ss Cst.; art. 18, al. 1 et 3 ConstC): Toute atteinte portée au droit fondamental à la protection des données doit être vérifiable devant un tribunal ou un autre organe indépendant.

Contrairement à l'article 14a LCPD en vigueur, la disposition est formulée de manière positive. Elle est adaptée à la législation fédérale.

Afin qu'un contrôle du niveau de protection des données ne soit pas nécessaire à chaque communication à l'étranger, le législateur cantonal prévoit (à l'instar de la Confédération) que le caractère adéquat du niveau de protection peut être assuré à certaines conditions.

Un niveau de protection adéquat est assuré par un traité international (lit. *a*), une décision d'adéquation du Conseil fédéral (lit. *b*) ou d'autres garanties appropriées (lit. *c*). La disposition correspond à ce que prévoit l'article 16, alinéas 1 et 2 LPD.

Lettre a

Par «traité international», on entend non seulement une convention internationale en matière de protection des données à laquelle l'État destinataire serait partie, comme le protocole d'amendement STE nº 108+ dont les exigences auraient été transposées par l'État partie dans son droit interne, mais aussi tout autre accord international qui prévoit un échange de données entre États parties et qui répond en substance aux exigences du protocole d'amendement mentionné. Si la communication se fait vers un pays de l'Union européenne, il est possible de partir du principe que le niveau de protection des données est adéquat, pour autant que toute transmission ultérieure des données à un État tiers soit exclue.

Lettre b

Un niveau de protection approprié peut en outre être assuré lorsqu'un État se trouve sur la liste positive du Conseil fédéral (lit. *b*). Conformément à l'article 16, alinéa 1 LPD, le Conseil fédéral constate dans une liste positive les États disposant d'un niveau de protection adéquat. La liste correspond à une des annexes de l'ordonnance fédérale. Il convient de noter que le contenu de cette liste, même s'il est actualisé régulièrement, ne doit pas toujours être exhaustif. L'absence du nom d'un État ne signifie pas forcément qu'il ne dispose pas d'un niveau de protection approprié; cette absence peut aussi indiquer que le Conseil fédéral n'a pas encore procédé à l'évaluation[57]. Cette disposition allège clairement la tâche des autorités, puisqu'il ne leur est plus nécessaire de vérifier qu'un État tiers offre un niveau de protection approprié lorsqu'il existe une décision d'adéquation du Conseil fédéral. Il s'agit là d'une simplification, qui tient donc compte de la motion Vogt.

S'agissant des États-Unis d'Amérique, la situation est la suivante: La CJUE a rendu un arrêt le 16 juillet 2020, dit «Schrems II», dans lequel elle constate que les États-Unis d'Amérique n'offrent pas de protection des données comparable à celle prévue par le droit européen. Elle a notamment retenu que, en vertu des réglementations internes de ce pays (Section 702 Foreign Intelligence Surveillance Act, FISA; Executive Order 12333), les autorités locales pouvaient accéder à des données à caractère personnel qui s'y trouvaient transférées. L'atteinte portée aux droits fondamentaux des personnes concernées a été jugée disproportionnée car l'accès aux données personnelles était illimité et il n'existait pas de moyens de protection juridique efficaces. Le Conseil fédéral a tenu compte de cette appréciation dans la mesure où il n'avait pas inclus les États-Unis d'Amérique dans sa liste positive jusque-là (annexe 1 de l'ordonnance fédérale sur la protection des données, entrée en vigueur le 23 septembre 2023).

[57] FF 2017 6565, p. 6658

Lors de communications de données personnelles vers les États-Unis d'Amérique, notamment lors de l'utilisation des services en nuage d'une entreprise étasunienne, les autorités devaient veiller à la garantie d'un niveau de protection adéquat par d'autres moyens (comme les clauses d'un contrat standard) et des mesures supplémentaires impératives (comme le chiffrement des données personnelles, lit. *c*) ou pouvoir se fonder sur l'une des circonstances justifiant une exception visées à l'alinéa 2.

Il est permis de recourir à des services en nuage pour le traitement de données en Suisse ou dans l'Union européenne même s'ils sont proposés par une entreprise contrôlée économiquement depuis l'étranger, à condition que d'autres mesures soient prises (clauses contractuelles, chiffrement, etc.) et que les données restent «physiquement» en Suisse ou dans l'Union européenne.

Désormais, un nouveau cadre garantit la sécurité des échanges de données personnelles entre la Suisse et les entreprises certifiées aux États-Unis d'Amérique: le Swiss-U.S. Data Privacy Framework. Telle est la conclusion du Conseil fédéral, qui a ajouté dans cette mesure le pays à la liste de ceux qui garantissent un niveau de protection des données adéquat et a fixé l'entrée en vigueur de la modification de l'ordonnance sur la protection des données au 15 septembre 2024. À partir du moment et pour toute la période où des entreprises étasuniennes certifiées figurent sur la liste de l'annexe 1 de l'ordonnance sur la protection des données, la communication de données personnelles dans ce cadre est admise selon l'article 15, alinéa 1, lettre *b* P-LCPD.

Lettre c

Un niveau de protection approprié peut aussi être atteint par d'autres garanties suffisantes (lit. *c*). Conformément au droit actuel et contrairement aux dispositions fédérales (art. 16, al. 2, lit. *b* à *e* LPD), la loi cantonale sur la protection des données renonce à mentionner chacune des garanties. Elles comprennent notamment les clauses de contrat approuvées par le PFPDT. Il faudra concrétiser les garanties suffisantes dans les dispositions d'exécution.

Pour l'adaptation de l'article 14, paragraphe 5 STE n° 108, l'article 17 STE n° 108+ prévoit une obligation d'informer l'autorité de protection des données lorsque la communication de données à l'étranger repose sur des garanties. Le droit actuel prévoit déjà une telle obligation (art. 14a, al. 3 LCPD). Au niveau fédéral toutefois, il a été décidé de renoncer à cette obligation d'informer: le parlement a supprimé la disposition lors des débats. Seule en est restée la possibilité d'informer, si demande en est faite et pour autant que la communication présente un lien direct avec la conclusion d'un contrat en faveur de la personne concernée ou alors dans la mesure où elle est nécessaire sur la base d'intérêts publics prépondérants dans le cadre de prétentions juridiques ou qu'elle a lieu pour protéger la personne concernée. Compte tenu du fait que l'autorité de protection des données peut de toute manière obtenir des renseignements en vertu de l'article 45, alinéa 2, lettre *a* P-LCPD, une règle explicite n'est pas nécessaire. Dans un souci d'harmonisation avec le droit fédéral, il est renoncé à l'obligation d'informer. Ainsi, un allègement du travail de l'autorité est possible, de sorte que le choix de ne pas reprendre la disposition sert à la mise en œuvre de la motion Vogt.

Alinéa 2

Des données personnelles peuvent être communiquées à l'étranger même si le niveau de protection adéquat n'est pas garanti. Il faut alors qu'une des conditions visées à l'alinéa 2 soit remplie. Par rapport à la législation actuelle, la disposition perd considérablement de son volume, puisque les règles étaient conçues pour les personnes privées et qu'il manquait des cas d'application pour les autorités.

Lettre a

La lettre *a* correspond à l'ancienne première phrase de la lettre *d*. L'existence d'un intérêt public prépondérant doit être attestée par les circonstances du cas d'espèce. Un intérêt purement hypothétique ne suffit pas. Par «sauvegarde d'un intérêt public prépondérant» on entend par exemple la sécurité intérieure de la Suisse ou d'un État tiers. En vertu de cette disposition, des données personnelles peuvent également être transmises à l'étranger dans le cadre d'actions humanitaires, par exemple lorsqu'il s'agit pour l'autorité de transmettre des données aux fins de recherche des personnes disparues dans une zone de conflit ou dans une région qui a subi une catastrophe naturelle.

Lettre b

La possibilité d'une communication des données à l'étranger est maintenue dans les cas où la personne y a explicitement consenti. Le consentement peut être donné par la personne concernée pour une ou plusieurs communications déterminées (voir aussi l'art. 4, al. 2, lit. *c* P-LCPD). Le caractère explicite découle de l'article 17 STE n° 108+. Cet adjectif signifie que le consentement doit clairement manifester la volonté de la personne concernée. La déclaration de volonté peut notamment avoir lieu dans la mesure où la personne coche une case ou opte activement pour certains paramètres techniques ainsi que par une autre déclaration. La même chose vaudrait pour des moyens d'expression non verbaux ou des mouvements qui, dans le contexte, sont des signes clairs. Lorsqu'un consentement exprès est requis, il ne peut pas être tacite. La personne concernée doit en particulier connaître le nom de l'État tiers et être informée des risques de la communication, notamment par rapport au niveau de protection des données de l'État étranger. Il faut reprendre aussi l'article 17, alinéa 1, lettre *e* LPD. Il permet des communications si la personne concernée a rendu ses données accessibles à tout le monde et ne s'est pas opposée formellement au traitement. La communication est aussi admise dans le pays aux mêmes conditions (art. 14, al. 1, lit. *b* P-LCPD).

Lettre c

La lettre *c* rend la communication de données à l'étranger possible lorsqu'elle est nécessaire pour protéger la vie ou l'intégrité physique ou psychique de la personne concernée ou d'un tiers. La teneur correspond à ce que prévoit actuellement l'article 14a, alinéa 2, lettre *e* LCPD hormis en ce qui concerne l'ajout «et qu'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable». L'adaptation se fonde sur la loi fédérale sur la protection des données. Obtenir le consentement de la personne concernée n'est par exemple pas possible lorsqu'elle souffre d'une incapacité physique ou qu'elle n'est pas joignable par les moyens usuels de communication.

Article 16 – Destruction, conservation et archivage

Cet article porte sur les points de contact et de recoupement entre la législation sur la protection des données et celle régissant l'archivage. Les données personnelles sont traitées pour l'accomplissement de tâches, mais le principe de proportionnalité commande qu'un tel traitement soit de durée limitée.

Il convient à ce sujet d'expliquer que le délai de conservation fixé par l'autorité selon l'alinéa 2 est une application générale du principe de la proportionnalité. Une fois ce délai passé, l'autorité doit détruire les données ou motiver pour chaque cas, selon l'alinéa 3, pourquoi elles doivent être conservées comme moyen de preuve ou de sûreté (lit. *a*) – c'est-à-dire pourquoi elles restent nécessaires dans le cadre de l'accomplissement de la tâche primaire, de la finalité initiale et de la même base juridique – d'une part, ou qu'il existe une nouvelle base juridique ou une nouvelle finalité justifiant la conservation au-delà du délai prévu (lit. *b*) d'autre part. La présente réglementation se rapporte donc au cycle de vie des données.

Selon l'archivistique moderne, les affaires ont un cycle de vie en trois phases (active, semi-active et inactive). Les phases ne se déroulent pas de manière strictement séquentielle, mais en partie de façon parallèle. Chaque phase est expliquée ci-dessous.

- La phase active débute avec l'ouverture d'une affaire et se termine à sa clôture. Durant cette phase, l'autorité traite les données personnelles dans un but déterminé. Ce but est conditionné par une tâche prévue par la loi dont l'accomplissement est le moteur du traitement de données et qui justifie ainsi ce dernier.
- La phase semi-active commence après la clôture d'une affaire et s'arrête après l'expiration du délai de conservation du dossier. L'affaire et les documents classés dans le dossier ne subissent plus aucune modification durant cette phase. L'accomplissement de la tâche originelle constitue toujours ce qui justifie le traitement des données; la finalité toutefois a changé. Le traitement n'a lieu que dans le but pour lequel les données personnelles sont conservées.
- La phase inactive correspond au versement aux archives des données à valeur archivistique qui ne sont plus utilisées. L'archivage implique un changement dans la finalité. Les données archivées servent les objectifs d'effet conformément à l'article 2 de la loi du 31 mars 2009 sur l'archivage (LArch)[58] et continuent d'être nécessaires à cette fin. L'accès aux données est autorisé uniquement aux fins prévues par la législation sur l'archivage.

Titre

L'article régit la conservation de données personnelles en plus de leur destruction et de leur archivage. Le titre est donc adapté pour en tenir compte.

Alinéa 1

L'alinéa 1 fixe le principe selon lequel il convient de détruire les données personnelles qui ne sont plus nécessaires. La nécessité des données est définie par la loi, plus précisément par le but poursuivi. Le but peut être en premier lieu le but du traitement dans le cadre de l'accomplissement d'une tâche légale (phase active, al. 1) et, dans un deuxième temps, la conservation (phase semi-active, al. 2 et 3) et la conservation durable prescrite par la législation sur l'archivage (phase inactive, al. 4).

Les données sont considérées comme détruites au sens de la disposition si l'état dans lequel elles se trouvent empêche toute probabilité de rapprochement avec la personne. L'anonymisation, tant qu'elle est efficace, est une méthode possible.

Alinéa 2

Par l'alinéa 2, le législateur oblige les autorités à déterminer un délai de conservation et à définir si et combien de temps des données personnelles sont à conserver lorsqu'elles ne leur sont plus utiles pour l'accomplissement de leurs tâches. La phase semi-active (phase de conservation) n'a lieu que si les données continuent d'être nécessaires, soit parce que l'autorité a fixé un délai de conservation, soit parce que la législation spéciale le prévoit. La réserve formulée à l'alinéa 2 se réfère au délai de conservation fixé par l'autorité. Il existe par exemple un délai particulier de ce type à l'article 26, alinéa 2 de la loi du 2 décembre 1984 sur la santé publique (LSP)[59]: les dossiers doivent être conservés au minimum pendant vingt ans.

Les délais de conservation laissent supposer, indépendamment des cas particuliers, que les données personnelles restent nécessaires pour la finalité admise légalement soit pour servir comme moyen de preuve ou de sûreté soit pour retracer l'accomplissement de la tâche. Le but de la conservation reste fondé sur la finalité première, c'est-à-dire l'accomplissement des tâches. Dans de nombreux cas, les délais de conservation sont fixés de manière normative

[58] RSB 108.1
[59] RSB 811.01

dans la législation spéciale, raison pour laquelle le droit en vigueur énonce une réserve, à l'alinéa 4, concernant des prescriptions de conservation spéciales. Cette réserve est déplacée de l'alinéa 4 à l'alinéa 2 en vue d'une amélioration de l'ordonnancement.

Alinéa 3

L'alinéa 3 sert à indiquer les conditions qui justifient la conservation au-delà du moment fixé par l'autorité selon l'alinéa 2 ou exigé aux termes de la législation spéciale (voir l'al. 2). Dans des cas d'espèce, l'autorité peut donc prouver que la nécessité des données personnelles perdure et qu'elles doivent par conséquent être conservées après les délais prévus.

Alinéa 4

En même temps, la réserve de l'alinéa 4, en faveur de la législation sur l'archivage, est reformulée et complétée. L'archivage est une finalité que la loi permet; les données devant être archivées ne doivent donc pas être détruites (voir l'al. 1). Il n'est donc plus renvoyé à la législation sur l'archivage à titre de réserve. L'alinéa crée plutôt un lien entre la législation sur la protection des données et celle portant sur l'archivage, soulignant ainsi que l'archivage ne déroge pas au principe de la suppression des données qui ne sont plus nécessaires (al. 1), mais constitue un autre but de traitement prévu par la loi.

Article 17 – Traitement à des fins ne se rapportant pas à des personnes

Le traitement de données personnelles pour les besoins de la statistique, de la planification ou de la recherche scientifique jouit de conditions beaucoup plus souples en matière de protection des données parce que la personne concernée ne compte en l'occurrence pas en tant qu'individu mais uniquement en tant qu'unité statistique anonyme. Comme les données personnelles perdent tout caractère individuel au cours du traitement, les droits fondamentaux de la personne concernée ne sont plus touchés.

À la différence du droit actuel, le titre, «Traitement à des fins ne se rapportant pas à des personnes», est formulé de manière plus neutre. La terminologie de la loi fédérale a été reprise, en français, après la procédure de consultation.

Alinéa 1

Quelques exemples d'utilisation dans un but qui est sans relation directe avec les personnes concernées sont fournis à l'alinéa 1: la recherche, la jurisprudence, la statistique et la planification. Les conditions du traitement correspondent à celles prévues aujourd'hui, bien que des modifications rédactionnelles aient été apportées.

Les données personnelles doivent être anonymisées ou pseudonymisées dès que le but du traitement le permet (lit. *a*). La teneur actuelle, selon laquelle les données personnelles peuvent seulement être utilisées «sans référence directe aux personnes intéressées», laisse place à la notion de pseudonymisation, reprise du règlement général sur la protection des données et de la directive (UE) 2016/680 et concorde avec la proposition du guide de la CdC. Dans ce cadre, les données personnelles sont réputées pseudonymisées lorsqu'elles ne peuvent plus être attribuées à une personne concernée précise sans informations supplémentaires. Ces informations supplémentaires doivent être conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne puissent pas être attribuées à une personne physique.

Par rapport à la disposition en vigueur, l'ajout de la précision «en cas de» met en évidence le fait qu'une publication des résultats n'est pas nécessairement attendue de l'autorité, mais seulement que si les résultats sont publiés, elle doit apporter la garantie que les personnes concernées ne sont pas identifiables à ce moment-là.

Les conditions des lettres *a* et *b* sont cumulatives.

Alinéa 2

L'autorité peut communiquer, à certaines conditions, des données personnelles à des tiers qui désirent les traiter à des fins ne se rapportant pas à aux personnes concernées. Les exigences supplémentaires fixées à l'alinéa 2 doivent être garanties par contrat ou, lorsque cela s'avère judicieux, par décision[60].

Elle a alors l'obligation d'anonymiser ou de pseudonymiser les données ainsi que d'imposer aux tiers les exigences relatives à la publication des résultats (lit. *a*).

Contrairement à ce que prévoit le droit en vigueur, les données peuvent être transmises à des tiers avec le consentement de l'autorité (lit. *b*), qui ne peut l'accorder que si existe la garantie que ces tiers traiteront aussi les données dans la seule mesure prévue par les conditions de l'article 17, alinéa 2.

Par contre, la sécurité des données doit être garantie par la ou le destinataire, comme jusqu'à présent (lit. *c*). La version allemande comporte par ailleurs une modification terminologique, qui remplace un terme désuet (*Datensicherung*) par le mot retenu à l'article 10 P-LCPD (*Datensicherheit*).

Les conditions des lettres *a* à *d* sont cumulatives.

7.3 Obligations des autorités et des tiers mandatés

Article 18 – Analyse des risques en cas de traitements répétés envisagés

Pour chaque traitement répété envisagé, l'autorité évalue elle-même les risques qu'il présente pour les personnes concernées (niveau 1, art. 18 P-LCPD). Si le risque est élevé, l'autorité procède à une analyse d'impact relative à la protection des données personnelles (niveau 2, art. 18, al. 3 et art. 19 P-LCPD). Comme dans la loi fédérale, les éléments qui constituent un risque élevé pour les personnes concernées ne sont pas réglés de manière exhaustive. Lorsqu'un grand nombre de personnes est en outre concerné, l'autorité soumet le traitement à l'autorité de protection des données compétente en vue de sa prise de position (niveau 3, art. 20 P-LCPD).

Alinéa 1

L'alinéa 1 régit l'analyse des risques. Le droit européen, plus précisément l'article 12 STE nº 108+ sur la modification de l'article 10, paragraphe 2 STE nº 108 et l'article 27 de la directive (UE) 2016/680, exige une analyse de l'impact du traitement de la part des autorités et, si des tiers sont mandatés, de la part de ceux-ci. Il s'agit essentiellement d'une auto-évaluation de l'autorité, qui consiste en un examen, sous l'angle du droit de la protection des données, des traitements de données personnelles répétés qui sont envisagés. L'analyse n'a pas lieu à chaque fois que des données personnelles sont traitées, raison pour laquelle la loi cantonale sur la protection des données évoque des traitements répétés envisagés, tandis que le droit fédéral parle de «traitement» ou d'«opérations de traitement». L'adjectif «envisagés» est ajouté et souligne le fait que l'analyse des risques doit avoir lieu avant la mise en service. Quant à l'adjectif «répétés», il met en évidence le fait que les traitements uniques ne sont pas concernés par l'analyse des risques.

L'analyse des risques ne connaît pas d'exigences formelles élevées. Il suffit d'une note dans le dossier du projet lorsque les traitements de données personnelles ne présentent pas de risque élevé pour les personnes concernées et qu'une analyse d'impact formelle n'est pas nécessaire. Le droit qui prévalait jusqu'à présent ne prévoyait pas explicitement une telle analyse, mais elle

[60] Voir l'art. 32 de l'ordonnance du 20 janvier 2021 sur la plate-forme des systèmes des registres communaux (sur les autorités dotées de la personnalité juridique)

devait déjà avoir lieu dans le cadre du contrôle préalable – une étape déjà obligatoire pour l'ensemble des autorités.

Dans le cadre de l'utilisation des TIC par l'administration cantonale, les autorités cantonales doivent déjà, en vertu l'ordonnance de Direction du 3 janvier 2011 concernant la sûreté de l'information et la protection des données (OD SIPD[61]), évaluer, durant la phase d'«analyse préliminaire», si le projet présente des exigences poussées en matière de sûreté de l'information et de protection des données (SIPD) à l'aide d'une analyse SIPD (art. 5, al. 1 à 4 OD SIPD et, dorénavant, art. 18 P-LCPD). Si l'analyse met en lumière des exigences poussées, un concept SIPD qui définit les mesures organisationnelles et techniques supplémentaires nécessaires est à élaborer durant la phase de «conception» par l'autorité (art. 5, al. 5 OD SIPD et, dorénavant, art. 19 P-LCPD). Sur ce point, une base est désormais inscrite dans la loi pour définir ce qui prévalait de toute façon déjà pour les projets informatiques de l'administration cantonale. La disposition ne prévoit ainsi rien de nouveau et ne pose pas d'exigences excessives. Il faut pouvoir partir du principe que l'ensemble des autorités sont capables de satisfaire à ces exigences sans charge supplémentaire considérable.

Alinéa 2

L'alinéa définit les conditions d'existence d'un risque élevé et en présence desquelles une analyse d'impact relative à la protection des données personnelles est obligatoire selon l'alinéa 3. Compte tenu des prises de position parvenues lors de la procédure de consultation, la liste n'est plus formulée de manière exhaustive. Le risque déterminant est celui qui existe sans que des mesures soient prises pour la protection des droits des personnes concernées (soit le risque brut). L'analyse d'impact doit exposer comment le risque peut être écarté ou ramené à un niveau résiduel supportable (risque net) par des mesures techniques et organisationnelles appropriées (voir l'art. 10, al. 1 P-LCPD).

D'après le droit européen, repris à l'article 22, alinéa 2 LPD, 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. Le droit cantonal doit intégrer cet élément. Ces aspects doivent donc être appréciés, en particulier lors du recours à de nouvelles technologies, et peuvent être à l'origine d'un risque élevé.

Un tel risque existe notamment dans le cas d'un traitement de données sensibles et d'une surveillance systématique de grandes parties du domaine public. (lit. *a* et *b*).

Alinéa 3

Si l'autorité constate lors de l'auto-évaluation que le projet présente un risque élevé, elle entreprend une analyse d'impact formelle.

Article 19 – Analyse d'impact relative à la protection des données personnelles

Conformément aux prescriptions européennes et à la réglementation de la Confédération, l'analyse d'impact relative à la protection des données personnelles doit comprendre au moins une description du traitement envisagé (lit. *a*), une évaluation des risques pour la personne concernée (lit. *b*) ainsi que les mesures de protection prévues (lit. *c*).

Les mesures déjà prises ou encore à prendre qui sont indiquées ont pour but d'empêcher toutes les conséquences négatives d'un traitement ou au moins de les restreindre. La limitation de l'accès aux données et d'autres mesures garantissant la sécurité des données en sont des exemples.

[61] RSB 152.040.2

Article 20 – Contrôle préalable

Alinéa 1

Si l'analyse de risques montre que le traitement des données envisagé présente un risque élevé pour la personne concernée, et qu'il est prévu de traiter électroniquement les données personnelles d'un nombre important de personnes, l'autorité le soumet avant son début à l'autorité de protection des données en vue de sa prise de position. La disposition s'appuie sur celle que le projet de loi fédérale sur la protection des données prévoyait pour le contrôle préalable. Du point de vue du canton, tous les traitements de données personnelles doivent en effet être soumis au contrôle préalable de l'autorité de protection des données lorsqu'il ressort de l'analyse de risques qu'il y a un risque élevé pour la personne, et pas seulement lorsqu'il existe un tel risque malgré les mesures prises par l'autorité. Sur ce point, la loi cantonale sur la protection des données s'écarte de la teneur de l'article 23 LPD.

L'évaluation des risques liée à l'analyse d'impact se fonde sur le droit actuel qui définit quand un contrôle préalable doit être mené. Par conséquent, les cas où un contrôle préalable est requis ne doivent pas changer avec la révision du droit. De plus, l'aspect quantitatif doit être souligné dans le droit cantonal («étendue», «à grande échelle» conformément à l'art. 22, al. 2 LPD). Ainsi, un contrôle préalable n'est obligatoire que si un grand nombre de données personnelles est traité. Selon la pratique actuelle, il n'y a de toute façon pas d'obligation en ce sens si le traitement concerne moins de 1000 personnes. Les dispositions d'exécution en concrétiseront l'idée.

Le contrôle préalable permet à l'autorité de protection des données d'agir de manière préventive et consultative. La démarche de l'autorité est ainsi plus efficace, puisque les possibles champs problématiques d'un point de vue de la législation sur la protection des données sont détectés à un stade précoce du traitement déjà et des solutions peuvent être directement trouvées.

Alinéa 2

Comme dans le droit en vigueur, les modifications importantes doivent être soumises au contrôle préalable. Les contours de ce qui constitue une modification importante seront définis par voie d'ordonnance.

Alinéa 3

L'article 23, alinéa 2 LPD prévoit un délai de deux mois durant lequel l'autorité de protection des données peut communiquer ses objections concernant le traitement envisagé. Du point de vue du canton, la pertinence d'un délai n'est que limitée, puisque les petits projets sont examinés bien plus rapidement, tandis que le contrôle préalable des grands projets se déroule le plus souvent en plusieurs étapes. Par conséquent, la loi n'impose aucun délai fixe, comme le guide pratique de la CdC le préconise. Néanmoins, le contrôle préalable ne peut pas durer indéfiniment; c'est pourquoi l'autorité de protection des données est tenue de le réaliser dans un «délai raisonnable».

Article 21 – Obligation d'inscrire au registre

L'article 24 de la directive (UE) 2016/680 oblige l'autorité à tenir un registre de toutes les activités des traitements. Le champ d'application de la directive se limite toutefois à la prévention et à la poursuite pénale ainsi qu'à l'exécution des peines. Une telle obligation ne pourrait donc être mise en œuvre que dans le domaine en question. La Confédération maintient l'existence d'un registre des fichiers (maintenant: des activités de traitement) et requiert de toutes les autorités qu'elles déclarent leur registre au PFPDT, qui tient un registre des activités de traitement de l'ensemble des organes fédéraux (art. 12 et 56 LPD).

Le registre des fichiers favorise la transparence: d'une part, la personne concernée peut s'informer des fichiers existants pour faire valoir ses droits et, d'autre part, il facilite le travail de l'autorité de protection des données. Il faut donc que le nouveau droit cantonal reprenne aussi, dans une forme modifiée, cet élément. Le travail qu'impliquait jusqu'à présent le registre sera réduit dans la mesure où seuls les fichiers contenant des données sensibles seront répertoriés. La charge assumée par les autorités s'en trouvera diminuée. La situation peut en outre s'avérer particulièrement délicate lorsque les autorités exploitent un profilage ou utilisent des systèmes de prise de décision algorithmiques (ou ce qui est communément appelé l'intelligence artificielle). Comme expliqué, les profilages ne posent pas nécessairement de problème quant aux personnes concernées. Il en va de même pour le recours à l'intelligence artificielle si bien que l'annonce se limite aux cas d'applications présentant un risque élevé pour la personne concernée.

La limitation ne vaut cependant pas pour le champ d'application de la directive (UE) 2016/680, puisqu'il existe là une obligation d'enregistrer les activités (voir le commentaire de l'art. 22 P-LCPD).

Les dispositions d'exécution prévoiront concrètement dans quelle mesure les autorités pourront annoncer d'autres fichiers pour qu'ils figurent au registre.

Alinéa 1

L'autorité cantonale de protection des données tient et met à jour un registre des fichiers cantonaux (voir aussi l'art. 42, al. 2 P-LCPD).

Alinéa 2

Pour tenir ce registre, l'autorité cantonale de protection des données a besoin que les autorités cantonales portent leurs fichiers à sa connaissance. L'alinéa 1 les y contraint. L'obligation d'annoncer s'accompagne de l'obligation de communiquer les changements. En plus des fichiers qui contiennent des données sensibles, les autorités annoncent également les profilages à risque élevé qu'elles exploitent et les systèmes de prise de décision algorithmiques utilisés présentant un risque élevé pour la personne concernée. Intelligence artificielle, algorithmes ou systèmes algorithmiques sont souvent considérés comme synonymes. L'intelligence artificielle au sens d'une machine capable de penser et d'agir d'elle-même «comme un être humain» n'existe pas pour l'heure et n'existera pas dans un avenir proche. En réalité, les systèmes de prise de décision sont conçus par des êtres humains et fonctionnent, à partir d'une analyse de données, en développant et proposant des solutions à des problèmes ou des domaines déterminés[62]. Lorsque notamment les systèmes de prise de décision algorithmiques disposent d'une marge de manœuvre dans la prise de décision et que l'action ne repose pas seulement sur des règles fixes, le risque qu'ils représentent pour les personnes concernées pourrait s'avérer élevé. La situation doit néanmoins être évaluée au cas par cas.

L'autorité cantonale de protection des données va créer un masque de saisie à l'intention des autorités cantonales. Elles pourront ainsi annoncer leurs fichiers ainsi que les profilages appliqués et les systèmes de prise de décision algorithmiques présentant des risques élevés, qui feront l'objet d'une publication après un contrôle de l'autorité cantonale de protection des données. L'obligation faite aux autorités est donc remplie selon les consignes de l'autorité de protection des données. Le registre aide la personne concernée à savoir où sont éventuellement traitées des données à son égard. La possibilité de s'informer constitue le point de départ qui permet à la personne concernée de faire valoir les droits que la législation sur la protection des données lui confère.

[62] Öktem, Rosa (2021), Algorithmische Entscheidungssysteme, menschenrechtliche Vorgaben und Entwicklungen auf internationaler Ebene. in: Deutsches Institut für Menschenrechte (éd.)

Alinéa 3

Les autorités de droit communal et celles des Églises nationales doivent tenir elles-mêmes leurs registres. L'aspect organisationnel est laissé à leur compétence. Il y a toutefois lieu de faire remarquer que des registres publics et détaillés sont susceptibles de limiter le nombre de demandes de renseignement.

Alinéa 4

Les différents éléments des fichiers feront l'objet d'une liste publiée par voie d'ordonnance. L'annonce permet néanmoins déjà de savoir qui exploite le fichier et quelles catégories de données personnelles sont concernées (type de données sensibles comme l'appartenance religieuse). Ainsi, la loi ne mentionne plus que le but, dont il est possible de déduire en général le cercle des destinataires.

Le but indiqué peut être, par exemple: «Examen du droit à la réduction des primes» ou «Profilage à risque élevé» ou «Développement de systèmes algorithmiques de prise de décision». Une liste des contenus sera fixée par voie d'ordonnance comme le prévoit également la loi fédérale sur la protection des données. Étant donné qu'il s'agira d'une ordonnance d'exécution, une délégation explicite de compétences législatives n'est pas nécessaire.

Conformément au droit actuel, les fichiers qui n'ont été constitués que pour une courte durée ou qui sont déjà publiés sous une autre forme ne sont pas inscrits au registre. Par courte durée, on entend deux ans au plus et les autres formes de publication correspondent, par exemple, au versement aux archives cantonales ou communales ou alors à la reproduction dans des annuaires accessibles au public. Une exception n'est cependant possible que si elle ne présente pas de risque pour les personnes concernées.

Article 22 – Obligation des autorités de poursuite pénale et des tribunaux pénaux de tenir un registre

L'article 24 de la directive (UE) 2016/680 exige que les autorités opérant dans les domaines de la poursuite pénale et de l'exécution des peines tiennent un registre de toutes les catégories d'activités de traitement. Les autorités de poursuite pénale et les tribunaux dotés de compétences dans le cadre de procédures pénales sont cités aux articles 22 et 23 LiCPM. Les autorités de poursuite pénale sont la Police cantonale et les autres organes de police du canton et des communes pour autant qu'ils exercent leurs fonctions dans le domaine de la poursuite pénale, d'autres personnes compétentes en vertu d'attributions de police que leur confère la législation spéciale, ainsi que le Ministère public. Les autorités qui ont des attributions judiciaires dans le cadre des procédures pénales sont la Cour suprême, le Tribunal cantonal des mesures de contrainte, le Tribunal pénal économique, le Tribunal des mineurs, les tribunaux régionaux et les tribunaux régionaux des mesures de contrainte.

Le registre se rapporte aux activités de traitement et contient des informations sur le but du traitement, les catégories de destinataires des données personnelles et les catégories de personnes concernées. Il serait par exemple possible de choisir l'intitulé «vidéosurveillance assortie d'un enregistrement des images» comme catégorie d'activité de traitement. Une liste des différents contenus sera édictée par la voie d'une ordonnance d'exécution, qui n'implique pas de délégation explicite de compétences législatives. Les exceptions à l'obligation sont réglées par le Conseil-exécutif, également par voie d'ordonnance. La disposition est à appliquer avec discernement. La charge de travail qu'elle représente devrait rester limitée, puisque les données doivent aujourd'hui déjà être saisies pour le registre des fichiers.

L'établissement d'un tel registre peut être considéré comme une mesure d'autorégulation en matière de protection des données. Les autorités se forgent ainsi une vue d'ensemble des données personnelles qu'elles traitent. Cependant, ce registre a aussi vocation à servir d'instrument de contrôle à l'autorité de protection des données.

Article 23 – Obligation d'informer lors de la collecte de données personnelles

La norme de l'article 4 OiDPD (principes du devoir d'informer lors de la collecte de données personnelles) doit être transposée dans la loi cantonale sur la protection des données.

Alinéas 1 et 2

Lors de la collecte de données personnelles, l'autorité est obligée de transmettre certaines informations en rapport avec le traitement des données aux personnes concernées. Jusqu'à présent, l'article 9, alinéa 4 LCPD ne prévoyait de devoir d'informer que pour les traitements de données se déroulant dans le cadre de questionnaires systématiques. La base légale et le but du traitement devaient être communiqués. L'article 13 de la directive (UE) 2016/680 fournit une liste détaillée des informations à transmettre (par. 1 et 2) et règle les exceptions pour lesquelles la communication des informations n'a pas lieu (par. 3 et 4). Dans ces circonstances, la limitation à la collecte systématique par des questionnaires, telle que visée à l'article 9, alinéa 4 LCPD, est trop restrictive et le catalogue des informations à communiquer est lacunaire. Il faut donc que le droit cantonal règle sur la base du droit européen et du guide pratique de la CdC

- la constatation du fait que le devoir d'informer vaut pour toutes les sortes de traitement des données personnelles,
- l'étoffement de la liste des informations à communiquer et
- les exceptions.

Il convient en particulier de noter que l'autorité devra désormais rendre les informations disponibles en tout temps, et non simplement quand les personnes concernées en font la demande. La personne concernée doit pouvoir obtenir ces informations sans avoir à les demander. Le but est qu'elle ait en sa possession toutes les informations dont elle a besoin pour faire valoir ses droits. L'alinéa 2 indique les informations requises *a minima*, comme l'exprime l'ajout de l'expression «au moins». Sont aussi désormais touchés par l'obligation d'informer les systèmes algorithmiques de prise de décision présentant un risque élevé pour la personne concernée dans un souci de transparence et d'adéquation avec l'obligation d'inscrire au registre. Le profilage est inféré à partir du but du traitement.

Des informations additionnelles peuvent s'imposer, par exemple sur la durée de conservation, lorsque l'autorité collecte des données sensibles.

L'obligation d'informer s'applique seulement dans la mesure où l'autorité «collecte» des données personnelles. Si elle acquiert de telles données sans l'avoir voulu ou par hasard, elle n'a pas de devoir d'informer la personne concernée. Il n'y a pas d'obligation en la matière concernant les modifications ultérieures, comme le changement des lieux de stockage, sauf si les données personnelles sont utilisées dans un autre but également; il s'agit alors d'une nouvelle acquisition.

Les modalités d'accomplissement du devoir d'informer sont laissées au libre choix de l'autorité. Dans la mesure où celle-ci traite des données sensibles, exploite un profilage à risque élevé ou utilise des systèmes algorithmiques de prise de décision présentant un risque élevé, elle satisfait à l'obligation qui lui est faite en publiant les informations dans le registre des fichiers. Si d'autres données ont été collectées directement auprès de la personne concernée, la publication sur un site Internet suffit. L'autorité doit veiller à ce que la personne concernée puisse effectivement prendre connaissance de l'information sans grande difficulté, mais pas à ce qu'elle s'informe réellement. Lorsque les données sont collectées auprès de tiers, une communication directe peut s'imposer.

Les exceptions sont réglées dans l'article suivant.

Article 24 – Exceptions à l'obligation d'informer

Alinéa 1

Il est possible de limiter l'obligation d'informer aux mêmes conditions que celles s'appliquant au droit d'accès, c'est-à-dire si la loi prévoit des obligations particulières de garder le secret et s'il existe un intérêt public ou privé prépondérant.

L'article 20 LPD cite explicitement un des intérêts publics: la sécurité publique. La loi cantonale renonce à la précision, conformément à ce que prévoit le guide pratique CdC (point 5.6).

Alinéa 2

Conformément au cadre légal européen, des exceptions à l'obligation d'informer sont possibles

- lorsque la personne concernée dispose déjà des renseignements (lit. *a*) ou
- lorsqu'ils découlent d'une base juridique au sens de l'article 4 P-LCPD (lit. *b*).

D'autres cantons précisent dans leur législation qu'il n'y a pas d'obligation pour les cas où le traitement est «expressément» prévu par un acte législatif. Quant à lui, le projet bernois prévoit, à l'article 24, alinéa 2, lettre *b*, que la base juridique doit permettre de déduire à un degré suffisant de précision l'autorité procédant au traitement, les données traitées et le but du traitement. Elle doit contenir les informations que l'autorité devrait sinon transmettre (art. 23, al. 2 P-LCPD). Les informations n'ont pas besoin de se trouver dans un article ou de figurer nécessairement dans la loi.

La réserve relative à la loi assure, par exemple, à la Police cantonale la possibilité de refuser de fournir des renseignements ou de ne pas communiquer les informations aux personnes concernées en cas de traitement de données relevant de mesures de contrainte au sens de la loi sur la police quand cela pourrait mettre en péril les enquêtes policières préliminaires (observation, enquête préliminaire secrète ou recherches secrètes).

Disposition non reprise

Par rapport au droit européen, un cas susceptible de donner lieu à une exception n'est pas repris, plus précisément là où les circonstances empêchent de respecter l'obligation d'informer ou impliquent des efforts disproportionnés. L'autorité peut publier les informations sur Internet; il est difficile de concevoir une situation où l'information impliquerait une charge de travail disproportionnée. L'autorité ne peut pas se fonder sur un intérêt public lorsqu'elle fait valoir la disproportion de la tâche.

Article 25 – Annonce des violations de la sécurité des données aux autorités de protection des données

À la différence de l'ordonnance portant introduction de la directive (UE) 2016/680 relative à la protection des données à caractère personnel, le législateur a préféré retenir «violation de la sécurité des données» pour le titre, plutôt que «violation de la protection des données», car seul l'aspect de la sécurité des données est abordé.

Alinéa 1

Selon le droit européen, l'autorité est tenue de notifier à l'autorité de protection des données les violations de la sécurité des données (art. 9 STE n° 108+ concernant la modification de l'art. 7, par. 2 STE n° 108 et art. 30, par. 1 de la directive (UE) 2016/680). Le terme «violation de la sécurité des données» est défini à l'alinéa 2. L'annonce doit avoir lieu dans la mesure du possible dans un délai de 72 heures à partir du moment où l'incident est connu. Contrairement à la législation fédérale, le délai de 72 heures est repris de la directive. L'autorité peut ainsi examiner le cas avant de l'annoncer et décider si une notification est absolument nécessaire. Le temps que

prennent les tiers mandatés à lui signaler une violation ne doit pas être imputé aux 72 heures dont dispose l'autorité.

En droit européen, le régime de l'annonce des violations de la sécurité des données dépend de règles différentes. L'article 9 STE nº 108+ concernant la modification de l'article 7, paragraphe 2 STE nº 108 prévoit que sont notifiées uniquement les violations susceptibles de porter «gravement atteinte» à la personne concernée (risque élevé), tandis qu'au sens de l'article 30, paragraphe 1 de la directive (UE) 2016/680 un risque commun suffit à motiver une annonce. La loi fédérale, quant à elle, l'exige seulement en cas de risque élevé pour la personne concernée. Il s'agit d'éviter l'annonce de violations insignifiantes. L'autorité doit évaluer dans tous les cas les conséquences de la violation pour la personne concernée[63]. L'obligation d'annoncer est aussi réglée différemment selon les cantons: pour Zurich et Lucerne, par exemple, elle suppose un risque élevé ou important pour la personne concernée, tandis que le canton de Bâle-Campagne renonce à l'obligation seulement si la violation de la sécurité des données ne présente probablement pas de risque pour les droits fondamentaux de la personne concernée. Le projet soumis à la procédure de consultation exigeait une annonce même si la violation ne présentait aucun risque élevé pour la personne concernée car l'obligation ne devait pas être l'exception mais la règle. L'objectif était que l'autorité de protection des données puisse soutenir l'autorité dans les tâches garantissant la sécurité des données le plus tôt possible et de façon globale.

La teneur de l'annonce à l'autorité de protection des données sera réglée par voie d'ordonnance (voir l'art. 24, al. 2 LPD).

Alinéa 2

L'alinéa 2 définit quand une violation de la sécurité des données est avérée au sens de la disposition. Cette disposition correspond dans sa teneur à l'article 5, lettre *h* LPD. L'adjectif «illicite» de la définition fédérale est remplacé par «sans autorisation». La formulation concorde ainsi avec celle retenue dans la loi sur la sécurité de l'information et la cybersécurité (LSIC)[64] qui doit être édictée au niveau cantonal. Un lien est ainsi établi avec le fait qu'une sécurité adéquate des données doit être garantie, par des mesures techniques et organisationnelles appropriées, lorsque leur traitement présente un risque pour la personne concernée (art. 10, al. 2 P-LCPD).

Il y a violation de la sécurité des données lorsque la disponibilité, l'intégrité ou la confidentialité des données sont affectées de manière imprévue par un traitement, par exemple,

- si le support de données est perdu ou volé (ordinateur portable, téléphone intelligent, disque dur, clé USB, etc.);
- si des tiers ou des membres du personnel qui n'y sont pas autorisés ont accès aux réseaux informatiques;
- si des données sont effacées à cause de coupures de courant, de pannes informatiques ou de catastrophes naturelles ou
- si des données personnelles sont portées à la connaissance de personnes non autorisées lorsqu'un courriel est envoyé à la mauvaise adresse.

Alinéa 3

En cas de sous-traitance, l'autorité doit être informée de la violation par les tiers mandatés. L'autorité devra régler contractuellement ce point.

[63] FF 2017, p. 6681
[64] RSB [à déterminer]

Article 26 – Annonce des violations de la sécurité des données à la personne concernée

Alinéa 1

Il faut distinguer l'annonce faite à l'autorité de protection des données de celle destinée à la personne concernée. En principe, la personne concernée ne doit pas être informée. Elle doit seulement l'être quand les circonstances l'exigent ou que l'autorité de protection des données le demande. Il existe une marge d'appréciation assez large.

Alinéa 2

Pour déterminer si l'annonce est obligatoire, il faut se demander si l'information peut réduire les risques de traitement abusif des données, en permettant notamment à la personne concernée de prendre les dispositions nécessaires pour se protéger (modification des données d'accès ou du mot de passe, p. ex.).

Article 27 – Exceptions à l'obligation d'informer la personne concernée

Alinéa 1

Il convient de renoncer à toute information de la personne concernée lorsque des obligations particulières de garder le secret prévues par la loi l'exigent ou que des intérêts publics ou privés prépondérants s'y opposent (voir aussi l'art. 24, al. 5, lit. *a* LPD). L'autorité ne dispose toutefois d'aucun pouvoir d'appréciation, raison pour laquelle la disposition n'utilise pas une formulation potestative. Un moyen moins drastique consiste en un report ou une limitation de l'information.

Alinéa 2

Il peut arriver qu'une personne concernée ne soit pas lésée par une violation de la sécurité des données (lit. *a*). Ce serait notamment le cas si les données divulguées en violation de la protection des données avaient été chiffrées par mesure de sécurité.

Des mesures prises ultérieurement peuvent aussi éventuellement garantir que le risque élevé ne soit selon toute probabilité plus susceptible de se matérialiser (lit. *b*). C'est par exemple le cas lorsqu'une personne qui a eu accès à des données sans y être autorisée peut être identifiée et qu'une convention écrite garantit par la suite que les données ne sont pas transmises et qu'elles sont supprimées.

Il n'est pas obligatoire d'informer la personne concernée lorsque l'information nécessiterait des efforts disproportionnés (lit. *c*). Ainsi en est-il lorsqu'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 qu'une communication publique est envisageable, pour autant qu'une annonce individuelle ne tende pas à améliorer sensiblement la situation de la personne concernée. Cette communication peut se faire, entre autres, par une publication sur le site Internet de l'autorité. L'annonce pouvant prendre la forme d'une publication officielle, rien ne la rend jamais impossible, de sorte que le projet s'écarte à cet égard de la loi fédérale.

7.4 Droits de la personne concernée

Article 28 – Droit d'accès

Alinéa 1

Le droit d'accès, c'est à dire de savoir quelles données à son sujet sont traitées par une autorité ou si cette dernière a mandaté un tiers pour le faire, est au cœur du droit de la protection des données. Il est à l'origine des autres droits et prétentions de la personne concernée.

Le droit d'accès complète l'obligation d'informer au sens des articles 23 et 24 P-LCPD. La personne concernée peut en apprendre plus que ce que l'autorité est tenue de lui communiquer si elle en fait la demande.

Alinéa 2

Le droit d'accès est un droit subjectif strictement personnel, 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 sa représentante légale ou de son représentant légal. Le fait que ce droit est strictement personnel a pour conséquence que nul ne peut y renoncer par avance.

Alinéa 3

L'autorité fournit les renseignements même en cas de traitement sur mandat.

Article 29 – Contenu et modalités des renseignements

Alinéa 1

La personne concernée reçoit les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la loi cantonale sur la protection des données et pour qu'ainsi la transparence du traitement soit garantie.

Les informations comprennent, d'une part, les données personnelles en tant que telles (lit. *a*) et, d'autre part, celles devant être transmises selon l'article 23 P-LCPD par l'autorité en cas de collecte de données (lit. *b*), auxquelles s'ajoutent la mention du délai de conservation (lit. *c*) et l'origine des données personnelles (lit. *d*). Les informations supplémentaires sont nécessaires au vu de l'article 11 STE n° 108+ concernant la modification de l'article 9, paragraphe 1, lettre *b* STE n° 108 et compte tenu de l'article 14, paragraphe 1, lettres *d* et *g* de la directive (UE) 2016/680.

La liste n'est pas exhaustive. La norme générale dans la phrase introductive permet à la personne concernée de demander d'autres informations qui sont nécessaires pour qu'elle puisse faire valoir ses droits et indispensables pour que la transparence du traitement soit garantie. Lorsque l'autorité traite des quantités importantes de données sur la personne concernée, elle peut au besoin demander que la personne concernée précise sur quelles données ou quelles opérations de traitement porte sa requête.

Alinéa 2

Le Conseil-exécutif règle les modalités du droit d'accès par voie d'ordonnance. Il faut par exemple qu'il pose comme principe le fait que les renseignements doivent être transmis par écrit, la forme électronique étant possible. Jusqu'à présent, le droit faisait une distinction entre l'accès et la consultation, alors que le droit de consultation est une forme de droit d'accès. Exceptionnellement, les renseignements peuvent être fournis lors d'une consultation des données personnelles sur place. Le délai autorisé pour fournir les renseignements est un autre exemple d'élément qu'il convient de régler.

La communication des données par une professionnelle ou un professionnel de la santé n'est pas réglée par la loi, à la différence de ce que prévoit le texte au niveau fédéral (art. 25, al. 3 LPD). La personne concernée peut au cas par cas accorder la possibilité à l'autorité d'assumer son devoir de renseigner par l'intermédiaire d'une tierce personne (voir l'art. 14, al. 1, lit. *b* P-LCPD). Les modalités précises seront réglées par voie d'ordonnance.

Article 30 – Restrictions au droit d'accès

L'article règle les restrictions au droit d'accès. Le principe du secret de fonction selon le droit du personnel exige des collaboratrices et collaborateurs de taire les faits dont ils ont eu connaissance dans l'exercice de leurs fonctions (voir l'art. 58 LPers)[65]. Il n'y a toutefois pas de violation du secret de fonction lorsqu'il existe une obligation légale de communiquer des données, comme dans le cas de renseignements sur ses propres données personnelles.

Sous le régime du droit en vigueur, un renseignement peut être refusé, limité ou différé par l'autorité dans la seule mesure où l'exigent une loi (sont ici visées des dispositions spéciales imposant un secret plus strict) ou des intérêts de tiers nécessitant une protection particulière. Il n'est pas fait mention des intérêts publics prépondérants, contrairement à ce qui est prévu pour la limitation de la consultation. Le rapport de 1985 renvoie toutefois à des intérêts publics également. Par similitude avec l'article 26 LPD, l'autorité refuse la communication d'un renseignement, la restreint ou la diffère lorsqu'un intérêt public ou privé prépondérant s'y oppose. Dans ces cas, elle est obligée de restreindre le droit d'accès.

Des exemples typiques d'intérêts publics sont la sécurité intérieure ou extérieure ou lorsque la communication d'un renseignement risque de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative (voir aussi l'art. 26, al. 2, lit. *b* LPD).

Des informations sur une personne identifiée peuvent, selon les circonstances, être liées à d'autres qui concernent une tierce personne; c'est le cas par exemple lorsqu'un tiers fait des déclarations au sujet d'une personne identifiée ou lors de dénonciations. Il faut alors procéder à une pesée des intérêts en présence.

Dispositions non reprises:

L'article 26, alinéa 1, lettre *c* LPD prévoit que l'autorité peut refuser, restreindre ou différer la communication des renseignements dans le cas où la demande d'accès est manifestement infondée notamment parce qu'elle poursuit un but contraire à la protection des données. Les procédures selon la loi cantonale sur la protection des données, notamment pour les demandes de consultations, sont régies par la loi sur la procédure et la juridiction administratives (LPJA). Selon l'article 45, alinéa 1 LPJA, les écrits de nature chicanière ou tendant à une mise en œuvre abusive de la procédure sont irrecevables. Par conséquent, il n'est pas nécessaire que la loi cantonale prévoie une réglementation spéciale à l'instar du texte fédéral.

Il n'est pas nécessaire de justifier d'un intérêt particulier pour invoquer le droit d'accès. L'autorité n'est donc pas habilitée à requérir, de manière générale, une motivation. Le Tribunal fédéral a néanmoins décidé qu'il y avait invocation abusive du droit d'accès, notamment parce qu'elle poursuit un but contraire à la protection des données, par exemple lorsque la personne dépose une demande pour se procurer des informations sur une (future) partie adverse et obtenir des preuves qui n'auraient pu l'être autrement[66].

La demande d'accès a un caractère manifestement procédurier lorsque le droit d'accès est invoqué de manière répétée sans motif valable ou que la personne adresse sa demande à une autorité dont elle sait pertinemment qu'elle ne traite pas de données la concernant. Dans ce cas non plus, l'autorité ne peut pas conclure à la légère à la nature procédurière de la démarche.

Article 31 – Droits en cas de traitement illicite

Alinéa 1

À la différence du texte de la Confédération, la loi cantonale sur la protection des données ne comporte pas la liste des trois droits de la défense traditionnels (actions en suppression ou en cessation de l'entrave et action en constatation de droit), mais nomme à titre d'exemple le droit

[65] RSB 153.01
[66] ATF 138 III 425, consid. 5.4 s.

de la personne concernée à faire rectifier les données personnelles inexactes, détruire les données personnelles traitées de façon illicite ou éliminer par tout autre moyen les effets du traitement illicite. L'action en constatation de droit est nommée expressément.

Il y a traitement illicite lorsque, par exemple, il ne repose sur aucune base légale, il est disproportionné ou sa finalité est incompatible avec le but originel du traitement. Le traitement de données personnelles inexactes est aussi illicite, puisque l'exactitude des données personnelles est un principe de la protection des données (art. 8 P-LCPD). Les effets du traitement illicite peuvent entre autres aussi être éliminés par un communiqué aux destinataires des données personnelles, par la publication de la rectification ou par des dommages-intérêts et une indemnité pour tort moral. En outre, la personne concernée peut demander le blocage de la communication de ses données personnelles sans que leur traitement ne soit forcément illicite (voir l'art. 33 P-LCPD).

Ces droits peuvent être invoqués par la personne concernée. La loi cantonale sur la protection des données renonce à l'obligation d'établir un intérêt digne de protection et diffère ainsi de la teneur de l'article 41, alinéa 1 LPD. En fin de compte, l'intérêt digne de protection découle du principe de la protection des données et serait toujours présent en cas de traitement illicite.

Alinéa 2

L'autorité porte le fardeau de la preuve concernant l'exactitude des données. Ce fardeau n'incombe pas à la personne concernée qui devrait prouver leur inexactitude. Cette règle est définie par le principe selon lequel les données personnelles doivent être correctes (art. 8 P-LCPD). Si l'exactitude des données déjà traitées ne peut être démontrée, il incombe en principe à l'autorité de les rectifier ou de les détruire. L'autorité supporte donc le fardeau de la preuve. Par contre, la demande de rectification doit être motivée par la personne concernée. Cette dernière peut, dans certaines circonstances, se trouver incapable d'apporter la preuve définitive des corrections proposées, alors que l'autorité, de son côté, ne peut assumer son mandat sans traiter les données. C'est alors pour ces cas qu'une mention du caractère litigieux est prévue (al. 3).

Alinéa 3

L'alinéa a fait l'objet d'une adaptation terminologique pour mieux correspondre à la teneur de l'article 41, alinéa 4 LPD: «mention du caractère litigieux» est le terme retenu à la place de «version contradictoire». Ainsi, lorsque ni l'exactitude ni l'inexactitude de données personnelles ne peut être définitivement établie, il est possible d'ajouter aux données la mention de leur caractère litigieux. Les données ne peuvent ensuite être transmises qu'accompagnées de cette mention.

Article 32 – Droit à la communication de la décision

Comme le veut le régime actuel, les droits de la défense comprennent le droit à la communication de la décision aux autorités et tiers désignés par la personne concernée pour autant qu'il existe un intérêt digne de protection.

Article 33 – Droit de blocage de la communication à des personnes privées

La personne concernée qui prouve un intérêt légitime peut s'opposer à ce que l'autorité communique les données personnelles qu'elle traite à des personnes privées (voir aussi l'art. 50, al. 2 LPJA). Il faut notamment penser aux réfugiées et réfugiés politiques qui se sentiraient menacés par des persécutrices et persécuteurs étrangers.

La communication ne peut toutefois pas être empêchée lorsque l'autorité est tenue, par des règles de la législation spéciale, de communiquer les données ou lorsque la personne privée ne peut pas, sans les données personnelles, exercer ses droits à l'encontre de la personne concernée.

Le contenu de l'article 13, alinéa 3 de l'actuelle LCPD, qui porte sur le blocage de la communication de données personnelles par le contrôle des habitantes et habitants se trouve dans une loi spéciale (voir le point 7.9.3).

7.5 Autorités de protection des données

Aujourd'hui, chaque commune et autre collectivité de droit communal dispose, pour son domaine, de sa propre autorité de surveillance qui assume le rôle d'autorité de protection des données. La présente révision doit offrir un cadre où les tâches de surveillance sont centralisées et la charge des communes s'en trouve allégée. Un nouveau modèle a été développé conjointement par l'autorité cantonale de protection des données, l'OACOT, l'ACB et le Directoire des préfectures, avec le concours de plusieurs communes. Sur la base de ce modèle, les tâches jusque-là attribuées aux autorités communales de protection des données doivent être transférées à l'autorité cantonale. Font exception les quatre communes les plus peuplées du canton (Biel/Bienne, Berne, Köniz et Thoune) et d'autres collectivités de droit communal. Le travail de l'autorité cantonale de protection des données se concentrera sur les prestations de conseil ainsi que sur l'accompagnement et sur la formation des autorités. Le niveau de protection des données doit s'en voir relevé et les ressources allouées permettront de gagner en efficience.

Les cantons organisent le domaine de la surveillance de la protection des données de manière bien différente, mais ils ne sont qu'un tout petit nombre à prévoir une surveillance obligatoire au niveau communal. C'est le cas notamment du canton de Saint-Gall. La solution d'une décentralisation n'est pas maintenue, puisqu'elle ne permet ni d'atteindre un niveau de protection accru ni d'utiliser les ressources avec efficience. L'option retenue, c'est-à-dire celle d'une centralisation partielle, a l'avantage d'éviter que l'autorité cantonale de protection des données ne soit accaparée dans son travail par les plus grandes communes principalement. Il faut ajouter que ces dernières disposent de services de surveillance professionnels et bien établis, qui garantissent aujourd'hui déjà un niveau élevé de protection des données. Dans le canton de Zurich, la solution retenue est similaire dans la mesure où seules la ville éponyme et Winterthour ont leur propre autorité de surveillance. Le reste des communes, contrairement à ce que le projet législatif bernois prévoit, peuvent choisir si elles gèrent une autorité qui leur est propre. Cette possibilité a été écartée dès le début du processus législatif, car le canton aurait couru le risque de voir une mosaïque de circonstances locales et des différences qualitatives dans la pratique en matière de protection des données. La variante mise en consultation augmente le niveau de protection des données, restant ainsi adéquate.

Article 34 – Statut

Alinéa 1

L'autorité cantonale de protection des données a le même statut que le Contrôle des finances: elle est autonome dans l'accomplissement de ses fonctions, n'est liée à aucune directive et est soumise uniquement à la Constitution et à la loi. Mais, contrairement aux tribunaux, elle fait partie de l'administration. L'indépendance de cette autorité ne doit toutefois pas conduire à une situation qui verrait cet organe se transformer en un «quatrième pouvoir» incontrôlé voire même à un «État dans l'État»[67]. Elle est donc une unité qui fait partie de l'administration et qui est subordonnée sur le plan administratif. Dans la mesure où son indépendance vis-à-vis de l'administration est garantie, l'autorité cantonale de protection des données ne doit pas jouer un rôle de «quatrième pouvoir». Il faut donc qu'elle soit rattachée à l'un des trois pouvoirs (législatif, exécutif, judiciaire); or l'exécutif (soit l'administration) est le seul pertinent. La solution idoine est

[67] Rapport du Conseil-exécutif sur la modification de la loi cantonale sur la protection des données (2008), pp. 14-15

d'assurer à l'autorité cantonale de protection des données le statut qu'a le Contrôle des finances, c'est-à-dire celui d'une unité indépendante au sein de l'administration. La loi sur l'organisation doit dorénavant la mentionner explicitement, comme elle le fait pour le Contrôle de finances (voir le commentaire du point 7.9.4).

Alinéa 2

Le statut reste inchangé par rapport à aujourd'hui, mais le nouvel article doit souligner l'autonomie de l'autorité. Le principe de l'indépendance de l'autorité est à reprendre tel que fixé à l'article 33a, alinéa 1 LCPD. De plus, le texte connaît une modification d'ordre rédactionnel visant une uniformatisation avec l'article 2, alinéa 2 de la loi du 17 mars 2022 sur le Contrôle des finances (LCCF)[68]. L'accomplissement du mandat de manière indépendante découle logiquement du principe susmentionné. Par conséquent, la loi n'a plus besoin de l'indiquer explicitement. L'autonomie de l'autorité de protection des données ne se limite pas à l'accomplissement de son mandat, mais porte également sur les questions organisationnelles et institutionnelles.

La précision concernant le fait qu'aucune directive ne peut être imposée à l'autorité de protection des données est aussi l'expression de son indépendance. N'est pas lié par des directives tout organe libre d'organiser ses activités. Cela signifie que l'autorité de protection des données est libre de ses choix dans les tâches qu'elle accomplit. Elle travaille ainsi sans avoir à tenir compte de directives spéciales et sans qu'on puisse dicter son comportement. L'objet de son travail ou la manière dont elle l'effectue ne peuvent pas lui être imposés par des directives. C'est aussi elle qui décide de son propre programme de contrôle. Naturellement, l'autorité de protection des données, comme tous les organes étatiques, est soumise à la Constitution et à la loi.

Alinéa 3

À ce jour, l'autorité de protection des données était rattachée administrativement à la Direction de l'intérieur et de la justice. Cet agencement résiste à l'épreuve du temps et présente plusieurs avantages: le rattachement à une Direction garantit que les messages puissent circuler jusqu'au Conseil-exécutif. Malgré le statut d'indépendance de l'autorité, ses requêtes peuvent et doivent être soumises au Conseil-exécutif par la directrice ou le directeur. De plus, l'état-major de la Direction l'aide dans la gestion du personnel, pour ce qui a trait entre autres à la saisie du temps de travail, à la modification des conditions d'engagement ou à la facturation. L'autorité de protection des données reste indépendante dans l'organisation de ses ressources et de ses activités.

Une autre option a été réexaminée avant d'être rejetée: le possible rattachement administratif au Bureau du Grand Conseil. L'idée n'a pas été retenue car l'autorité n'exerce pas de fonction parlementaire. Elle n'entretient pas non plus de contacts réguliers avec le Grand Conseil; elle est seulement tenue de soumettre un rapport à l'organe d'élection une fois l'an (art. 50 P-LCPD). Sous l'angle organisationnel, elle fait partie de l'administration, non pas du pouvoir législatif (voir le commentaire de l'al. 1). Une telle restructuration l'amènerait par ailleurs à perdre la possibilité d'échanger des informations avec le pouvoir exécutif, qui pour l'heure garantit des échanges caractérisés par un faible niveau de contraintes et d'exigences.

Au fond, un rattachement à la Chancellerie d'État serait une solution envisageable, à même de permettre aussi l'accès au Conseil-exécutif. Pour des raisons pragmatiques et dans une volonté de mise en œuvre de la motion Vogt, le présent projet propose de conserver l'ordre actuel, soit un rattachement administratif à la Direction de l'intérieur et de la justice. Un réordonnancement impliquerait une charge administrative et financière et n'apporterait apparemment aucune plus-value.

[68] RSB 622.1

Article 35 – Direction

Alinéas 1 et 2

Selon les prescriptions européennes, la déléguée ou le délégué à la protection des données doit disposer des qualifications, des connaissances et de l'expérience dans le domaine de la protection des données qui sont requises par l'accomplissement des tâches. Ces exigences sont dorénavant fixées à l'alinéa 2. La condition portant sur la compétence dans les langues officielles est légèrement modifiée; l'adaptation est de nature rédactionnelle.

Alinéa 3

La période de fonction de la déléguée ou du délégué à la protection des données est de quatre ans. L'attribution du poste fait suite à une élection (art. 36, al. 1 P-LCPD). Cette personne n'est donc pas une employée, mais un membre d'autorité à titre principal. Le renvoi à la législation sur le personnel sert à faciliter l'accès à l'information.

Article 36 – Élection et réélection de la déléguée ou du délégué à la protection des données

Alinéa 1

Depuis la modification législative de 2008, ce n'est plus le Conseil-exécutif qui désigne la déléguée ou le délégué à la protection des données, mais le Grand Conseil qui l'élit sur proposition du Conseil-exécutif.

Le processus électif n'est pas le même d'un canton à l'autre. Jusqu'à présent, la désignation est le fait du pouvoir exécutif dans la plupart des cas, parfois sous réserve de l'approbation de l'organe législatif. Le fait de confier le soin de l'élection au pouvoir législatif renforce en revanche l'indépendance de la déléguée ou du délégué à la protection des données, puisqu'on ne se retrouve pas dans la situation où le choix revient à l'entité contrôlée. L'implication conjuguée des deux organes garantit une représentation équilibrée des différents intérêts, raison pour laquelle les deux pouvoirs doivent continuer à participer à préparer l'élection (voir l'art. 37 P-LCPD).

À l'inverse de ce qui vaut pour la chancelière ou le chancelier ainsi que pour la secrétaire générale ou le secrétaire général du Grand Conseil, la déléguée ou le délégué n'a pas de mandat politique. La période de fonction n'a pas nécessairement besoin de correspondre à une législature. Il en va de même par exemple pour la cheffe ou le chef du Contrôle des finances (art. 3 LCCF). Lors de la révision, il a toutefois été souhaité, pour des raisons pratiques, que la période de fonction et la législature se recoupent, ce que les dispositions transitoires établissent (voir le commentaire de l'art. 60 P-LCPD).

Alinéa 2

Une réélection est déjà possible aujourd'hui. Il convient de continuer à renoncer à fixer une limitation du nombre de mandats. D'une part, il est indispensable d'avoir une certaine expérience et de disposer d'un réseau au sein de l'administration pour l'exercice de la charge; d'autre part, la personne élue doit se soumettre tous les quatre ans à une procédure de réélection.

Article 37 – Commission électorale

Contrairement à la proposition du Conseil fédéral, l'article 43, alinéa 1 LPD prévoit que l'Assemblée fédérale (Chambres réunies) élit la préposée ou le préposé. La Commission judiciaire de l'Assemblée fédérale prépare les propositions d'élection ainsi que les propositions concernant la révocation (art. 2 du projet d'ordonnance de l'Assemblée fédérale concernant les rapports de travail du chef du Préposé fédéral à la protection des données et à la transparence)[69].

[69] FF 2022 348

Depuis la révision partielle de 2008 de la loi cantonale sur la protection des données, la surveillance de la déléguée cantonale ou du délégué cantonal à la protection des données incombe à la Commission de gestion (Commission de haute surveillance auparavant). C'est à elle aussi qu'il revenait de préparer une proposition en vue de l'élection. En 2013, lors de la révision de la loi sur le Grand Conseil et du règlement s'y rattachant, le législateur a transféré l'attribution de préaviser la candidature proposée à la Commission de justice, un changement décrit comme logique compte tenu des tâches qu'elle assumait déjà en rapport avec l'élection des juges[70]. De plus amples explications ne sont pas fournies à ce sujet. Concernant l'élection de la chancelière ou du chancelier, il appartient au Bureau du Grand Conseil d'enregistrer les candidatures proposées (voir l'art. 31, al. 2 du règlement du Grand Conseil du 4 juin 2013 [RGC][71]). S'agissant de la cheffe ou du chef du Contrôle des finances, l'élection relève du Grand Conseil, qui se fonde sur la proposition du Comité Contrôle des finances; ce comité se compose, pour cette élection, des présidentes ou présidents de la Commission des finances et de la Commission de gestion, de la directrice ou du directeur des finances et d'un autre membre du Conseil-exécutif (art. 34, al. 1 LCCF[72]). Autrement dit, cette élection est préparée par un organe où règne la parité entre le pouvoir exécutif et le pouvoir législatif. Le statut de la déléguée ou du délégué à la protection des données est comparable à celui de l'organe du Contrôle des finances, ce qui ressort désormais de la législation d'organisation (voir le point 7.9.4). L'organe d'élection connaît une composition similaire. Aucun siège n'est donc prévu pour les communes. Il faut aussi dire qu'une sur-représentation de l'organe exécutif serait difficilement conciliable avec le concept d'indépendance sur le plan fonctionnel.

Alinéas 1 et 2

La candidature proposée par le Conseil-exécutif pour l'élection de la déléguée ou du délégué à la protection des données est actuellement préavisée par la Commission de justice (art. 38, al. 2, lit. *d* RGC). À présent, l'organe législatif ne participe pas à la préparation de l'élection. Or un processus sans heurts dépend de l'implication des parlementaires dans la sélection des candidates et des candidats, ainsi que de la possibilité de s'exprimer sur leurs qualifications. La composition de la commission électorale ressemble à celle du comité préparant l'élection de l'organe du Contrôle des finances.

Pour le moment, la proposition est soumise à la Commission de justice, qui la préavise à l'intention du Grand Conseil. Une telle consultation préalable n'est plus nécessaire dès lors qu'une commission électorale composée de membres de l'exécutif et du législatif doit être spécialement instituée. Il convient donc d'abroger l'article 38, alinéa 2, lettre *d* RGC, prévoyant le préavis de la Commission de justice. À l'avenir, la candidature proposée sera déposée auprès du Bureau du Grand Conseil, selon la procédure en place pour l'élection de la chancelière ou du chancelier et aussi pour l'organe du Contrôle des finances (art. 31, al. 2 et art. 82, al. 1, lit. *b* RGC). Les actes législatifs de rang inférieur ne peuvent pas faire l'objet d'une adaptation à titre de modification indirecte (parallélisme des formes). La modification du règlement du Grand Conseil fait donc l'objet d'un projet législatif distinct.

La réélection aussi est proposée par la commission électorale. Les membres de cette dernière peuvent être consultés par écrit si elle n'est pas contestée.

L'organe d'élection peut recourir aux conseils de tiers. Il est notamment envisageable d'impliquer la chancelière ou le chancelier ou de prendre l'avis de l'ACB lors d'une nouvelle nomination.

[70] Rapport sur la loi sur le Grand Conseil (LGC) et sur le règlement du Grand Conseil (RGC) du 3 décembre 2012, commentaire de l'article 38, p. 43.
[71] RSB 151.211
[72] RSB 622.1

Article 38 – Autorité de surveillance de la déléguée ou du délégué à la protection des données

Alinéa 1

L'alinéa 1 reprend l'article 38, alinéa 1, lettre *d* de la loi du 16 septembre 2004 sur le personnel (LPers)[73]. Selon cet article, la Commission de gestion surveille la déléguée ou le délégué à la protection des données. Il s'agit de respecter le principe consistant à formuler un acte de la manière la plus complète possible. La question de savoir si la Commission de gestion devait exercer la haute surveillance plutôt que la surveillance a été discutée. Toutefois, un manque de cohérence par rapport à la législation sur le personnel en découlerait. Une adaptation du texte législatif en ce sens a donc été écartée. De plus, l'autorité cantonale de protection des données exerce déjà la haute surveillance sur les autorités communales et ecclésiales du domaine; l'utilisation de cette terminologie dans deux contextes différents doit être évitée.

Alinéa 2

L'indépendance de la déléguée ou du délégué est ici une nouvelle fois soulignée; la Commission de gestion ne peut lui donner des instructions (voir le commentaire de l'art. 34, al. 2 P-LCPD). La surveillance dont fait l'objet la déléguée ou le délégué à la protection des données doit correspondre au contrôle que connaissent les tribunaux. Cela signifie notamment qu'un contrôle de l'activité dans sa teneur est exclu, qu'il se rapporte à l'opportunité, à la légalité, à la manière d'exercer l'activité ou au domaine, tout particulièrement à l'évaluation de questions relevant de la protection des données. Par analogie à ce qui prévaut pour les tribunaux dans la législation sur le Grand Conseil, les droits de la Commission de gestion découlent en particulier du chapitre 4 de la loi sur le Grand Conseil. L'activité de surveillance se limite à la déléguée ou au délégué et ne s'étend certainement pas au reste du personnel de l'autorité de protection des données.

La Commission de gestion a la possibilité de lancer une procédure de révocation au sens de l'article 41 LPers en cas de violations graves du devoir de fonction. Une révocation peut être proposée si, pour cause d'incapacité, de performances durablement insuffisantes, de manquements graves ou répétés aux obligations professionnelles ou pour un autre juste motif, il paraît inacceptable que la personne concernée continue d'exercer ses fonctions. Cette prescription tient suffisamment compte de l'indépendance exigée concernant l'autorité de protection des données.

Article 39 – Budget et plan intégré mission-financement

Comme c'est déjà le cas aujourd'hui, l'autorité cantonale de protection des données dispose d'un budget qui lui est propre et sur lequel ni le gouvernement ni l'administration n'ont d'influence. Le budget de l'autorité cantonale doit par conséquent être intégré au budget cantonal, ce qui incombe à l'administration. Le Conseil-exécutif doit pouvoir continuer à commenter le budget. La disposition est rédigée de sorte à présenter une cohérence avec l'article 7 LCCF.

Article 40 – Gestion financière

Les dispositions sur la gestion financière (art. 33a, al. 4 et art. 33b LCPD) sont réunies en un article et rédigées pour être similaires à celles de la législation sur le Contrôle des finances. La gestion financière dépend, comme aujourd'hui, de la législation sur les finances.

L'autorité cantonale de protection des données dispose elle-même des moyens qui lui ont été alloués par le budget. Ces ressources peuvent être affectées à l'engagement de personnel mais aussi à d'autres fins, telles que le paiement de prestations de spécialistes. Dans ce contexte,

[73] RSB 153.01

c'est à dessein qu'on a renoncé à exiger la conclusion d'une convention de prestations. Une telle convention contreviendrait en effet au principe de l'indépendance de l'autorité.

La loi continue de prévoir clairement que l'autorité cantonale de protection des données tient un compte spécial et que le Grand Conseil règle les structures comptables ainsi que la tenue des comptes par voie de décret, à savoir le décret du 1er février 2011 sur le compte spécial du Bureau cantonal pour la surveillance de la protection des données (DCSPD)[74].

Article 41 – Autorité de protection des données de droit communal et des Églises nationales

L'autorité cantonale de surveillance est renommée autorité cantonale de protection des données et sa fonction est renforcée. Diverses tâches relevant de la surveillance qui étaient effectuées jusqu'à présent par les communes et d'autres collectivités de droit communal seront reprises par l'autorité cantonale de protection des données (art. 43, al. 2 P-LCPD). Seules les communes et autres collectivités de droit communal comptant plus de 25 000 habitantes et habitants ou membres ainsi que les Églises nationales et leurs entités régionales disposeront d'une autorité de protection des données qui leur est propre et qui exerce les activités prévues par la loi cantonale sur la protection des données. Les communes concernées sont Biel/Bienne, Berne, Köniz et Thoune, fortes d'une population de plus de 25 000 personnes (voir aussi le point 3.6).

La loi prescrit que les communes fixent dans un règlement les modalités d'élection et d'organisation de leur autorité de protection des données étant donné qu'il s'agit de normes fondamentales relevant du droit de l'organisation (al. 2).

Article 42 – Tâches

Alinéa 1

Cet article résume en une liste condensée toutes les tâches des autorités de protection des données. L'article 42 et les suivants valent également pour les autorités de protection des données de droit communal et des Églises nationales.

Les autorités de protection des données soutiennent les autorités dans l'application du droit de la protection des données. Les tâches principales de ces autorités consistent à donner des conseils et à veiller à la bonne application des dispositions en matière de protection des données, notamment concernant la sécurité des données. Les conseils visent à faire en sorte que les autorités traitent les données personnelles en respectant les normes de protection des données; la surveillance permet de contrôler si elles respectent les dispositions relevant de la protection des données. L'accent est mis sur les conseils. La liste des tâches est restructurée. Les tâches liées à la surveillance sont indiquées aux lettres *a* à *c* (le contrôle préalable précède le traitement des données effectif), tandis que les activités de conseil sont précisées aux lettres *d* à *h*. Pour le reste, il s'agit de travail de relations publiques et de publication du registre des fichiers. Dresser l'inventaire de toutes les tâches implique certes une redondance avec quelques parties du texte de loi, mais ne manque pas de logique. En effet, les autorités de protection des données ne disposent en général pas de leur propre ordonnance ou règlement d'organisation. Lors de la collaboration avec d'autres autorités, la liste des tâches permet d'expliquer le champ d'action de l'autorité de protection des données.

Lettre a

L'autorité de protection des données agit soit d'elle-même et contrôle le respect de la loi selon le programme qu'elle s'est fixée de manière autonome, soit sur dénonciation (voir l'art. 45 P-LCPD). L'objectif de la surveillance est de déceler les potentielles irrégularités et d'indiquer là

[74] RSB 620.03

où des mesures sont nécessaires pour que l'état conforme au droit puisse être rétabli. La surveillance de la sécurité des données fait partie de la surveillance des dispositions relevant de la protection des données, raison pour laquelle une tâche à proprement parler n'a pas à être définie.

Lettre b

Le contrôle préalable constitue une autre tâche principale des autorités de protection des données. Par opposition au droit actuel, le renvoi explicite à l'article est supprimé car il est possible de le déduire du texte de loi. Le contrôle préalable se rapporte au traitement systématique envisagé de données personnelles qui présente un risque élevé pour les des personnes concernées, en raison des données personnelles traitées ou du type de traitement, et qui touche un vaste nombre de personnes (voir l'art. 20 P-LCPD). Contrairement à la surveillance, les contrôles préalables ne portent pas sur un traitement de données personnelles qui a ou a eu lieu, mais sur un traitement qui aura lieu.

Lettre c

Selon les exigences de l'article 52 de la directive (UE) 2016/680, «toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle unique, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation des dispositions adoptées en vertu de la […] directive». Il n'y a aucune raison de supposer, et le guide de la CdC atteste d'un avis concordant, que cette prescription impose un système allant au-delà des dénonciations faites à l'autorité de surveillance que le droit cantonal prévoit (art. 101 LPJA). Il n'y a de ce fait pas lieu d'introduire un nouveau moyen non juridictionnel qu'il serait possible de faire valoir devant l'autorité de protection des données. Aussi la lettre *c* correspond-elle à une contrainte imposée aux autorités de protection des données. Ces autorités doivent communiquer aux personnes dénonciatrices le résultat de leurs investigations dans un délai de trois mois (voir l'art. 45, al. 4 P-LCPD).

Lettre d

Le rôle de l'autorité de protection des données est surtout de dispenser des conseils. Elle conseille les autorités dans l'application de la loi, mais fournit aussi aux personnes concernées des renseignements sur leurs droits. Elle tient donc lieu de courroie de transmission entre autorités et personnes concernées, raison pour laquelle les deux tâches sont réunies.

Lettre e

Le droit d'accès de la personne concernée peut dans des cas déterminés, notamment en raison d'intérêts publics ou privés prépondérants, être refusé, limité ou différé (cf. art. 30 P-LCPD). En pareilles circonstances, les autorités de protection des données compétentes défendent les droits des personnes concernées.

Lettre f

Par projets d'acte législatif, on entend les projets de loi ou d'ordonnance ainsi que les projets de modification législative. Les principales mesures qu'il convient de garder à l'esprit sont notamment les dispositions prises pour garantir la sécurité informatique, les enquêtes, la création de processus et leur réagencement comme, par exemple, l'émission de certificats électroniques. Il existe une restriction pour les projets d'acte législatif et les mesures des communes et d'autres collectivités de droit communal qui n'ont pas d'autorités de protection des données propres (voir l'al. 3).

Lettre g

À la demande des instances de décisions ou de recours, les autorités de protection des données prennent également position sur des questions touchant à la protection des données.

Lettre h

Les autorités de protection des données sont en outre obligées de collaborer avec d'autres autorités de surveillance et de fournir une entraide administrative (voir l'art. 49 P-LCPD).

Lettre i

Les autorités de protection des données informent le public de manière périodique par la publication d'un rapport d'activité d'une part, et lorsque cela s'avère nécessaire, d'autre part, notamment s'il en va de l'intérêt général (voir l'art. 50 P-LCPD).

Alinéa 2

L'autorité cantonale de protection des données tient et publie aussi le registre cantonal des fichiers (voir l'art. 21 P-LCPD).

Alinéa 3

Pour des raisons pratiques, l'autorité cantonale de protection des données ne s'exprime que sur certains projets d'acte législatif et d'autres mesures des communes et collectivités de droit communal ne disposant pas de leur propre autorité de protection des données. Le règlement d'organisation et une partie des autres actes législatifs communaux sont soumis à l'examen préalable de l'OACOT, qui peut prendre position sur des questions de protection des données de rang inférieur. L'office peut consulter l'autorité cantonale de protection des données s'il le souhaite.

Article 43 – Surveillance en général

L'autorité de protection des données surveille le traitement de données personnelles opéré par les autorités. Naturellement, la surveillance se limite aux traitements entrant dans le champ de compétences de l'autorité de protection des données.

Article 44 – Secret de fonction

Le droit qu'a l'autorité de protection des données d'exiger des renseignements de la part d'autorités, indépendamment des obligations de garder le secret, implique en contrepartie qu'elle s'assujettisse au même titre qu'elles à leur obligation de garder le secret.

Article 45 – Contrôle du respect des dispositions en matière de protection des données

En vertu de la directive (UE) 2016/680 et du protocole d'amendement STE n° 108+, la déléguée ou le délégué à la protection des données obtient des compétences de contrôle plus vastes qu'auparavant. L'élargissement de ces compétences doit être inscrit dans le droit cantonal. L'article 35 LCPD, extrêmement dense dans sa version en vigueur, est divisé en trois articles: surveillance du respect des dispositions en matière de protection des données (art. 45 P-LCPD; actuellement: méthode de travail et procédure), recommandations (art. 46 P-LCPD) et mesures administratives (art. 47 P-LCPD).

Alinéa 1

Avant la mise en service des produits, l'autorité de protection des données examine les projets informatiques développés sous l'angle de la conformité à la protection des données, y compris de la sécurité des données. Cet examen a lieu dans le cadre du contrôle préalable au sens de l'article 20 P-LCPD. À la différence du contrôle préalable (qui consiste pour l'autorité de protection des données à collaborer avec les autorités pour déterminer la conformité de l'état à venir avec les dispositions en matière de protection des données et en termes de sécurité des données), l'autorité de protection des données examine également les produits déjà mis en service (examen de la situation actuelle). L'examen est mené par l'autorité de surveillance en vertu du programme de contrôle qu'elle s'est fixée ou à la suite d'une dénonciation relevant du droit de la surveillance.

Alinéa 2

Cet alinéa décrit la forme que prend la surveillance. Le droit en vigueur se contente de mentionner la collecte d'informations, l'accès aux documents et la possibilité d'effectuer des visites; l'ajout concernant le fait de recueillir des preuves et d'entreprendre d'autres démarches de contrôle est donc nécessaire.

En toute logique, les exigences en matière de preuve varient selon les utilisations: elles sont d'autant plus élevées que l'application est significative et que ses répercussions sont importantes. Les instruments permettant de mesurer le respect des dispositions sur la protection des données sont, par exemple, les systèmes de gestion de la protection des données (SGPD) ou les audits relevant du droit de la protection des données. Les SGPD répondent aux exigences des normes ISO sur le management de la qualité (ISO 9001) et sur la sécurité de l'information (ISO 27001). Une autre solution envisageable serait l'élaboration d'un simple rapport présentant la mise en œuvre des mesures. Le contrôle préalable mené par l'autorité de protection des données (art. 20 P-LCPD) et la procédure de mise en œuvre de la sécurité de l'information et de la protection des données (SIPD) ne constituent toutefois pas des preuves suffisantes. Ces instruments interviennent plutôt avant le traitement des données (détermination de l'état à venir). Or il faut en l'occurrence prouver que le traitement de données personnelles correspond bien à l'état défini lors du contrôle préalable.

L'examen a lieu d'habitude lors d'un audit. Une évaluation standardisée de la gestion des données personnelles se déroule dans ce cadre. Il s'agit de contrôler si les dispositions en matière de protection des données sont respectées durant les processus de traitement étudiés ou, par exemple, si les droits des personnes concernées sont garantis. Le contrôle peut en outre être l'occasion de vérifier si les données personnelles sont protégées par des mesures techniques et organisationnelles appropriées au vu du risque pour la personne concernée (voir l'art. 10 P-LCPD).

Les autres compétences de l'autorité de protection des données et la procédure déclenchée par la constatation de manquements découlent des articles suivants.

Alinéa 3

Par rapport au droit actuel, le fait que l'autorité est obligée de collaborer dans le cadre des démarches de contrôle n'a pas changé.

Alinéa 4

Aucune prescription ne définit le délai de traitement que l'autorité de protection des données doit respecter pour les dénonciations. L'article 34, alinéa 2 LCPD en vigueur se limite à obliger de manière générale l'autorité en question à informer les personnes concernées. Il existe par contre des directives pour le traitement des dénonciations à l'autorité de surveillance, édictées par le Conseil-exécutif le 14 novembre 2012 (ACE n° 1616). Selon le point 3 de cet ACE, les dénonciations à l'autorité de surveillance doivent généralement être traitées dans un délai maximal de six mois, sous réserve d'investigations particulièrement complexes.

Selon l'article 53, paragraphe 2 de la directive (UE) 2016/680, «[…] toute personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de [protection des données][…] ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article 52». Ce délai de trois mois doit être transposé dans le droit cantonal. Il ne vaut pas pour toutes les dénonciations à l'autorité de surveillance au sens de l'article 101 LPJA, mais seulement pour celles adressées à l'autorité de protection des données. Contrairement aux cas de dénonciation régis par l'article 101 LPJA, l'autorité de protection des données ne fournit pas que des informations sur la liquidation de la procédure; elle renseigne également sur le résultat de ses investigations.

Article 46 – Recommandations

Le système actuel, qui offre seulement la liberté à l'autorité de protection des données de faire une recommandation sous la forme d'une proposition motivée, ne suffit plus au vu des prescriptions européennes. L'autorité de protection des données est habilitée à rendre des décisions (voir l'art. 47 P-LCPD). Il doit toutefois rester possible pour elle de faire part de ses recommandations à l'autorité.

Du fait de l'obligation de motiver, l'autorité a l'occasion de prendre position sur les recommandations, ce qui lui garantit le droit d'être entendue selon l'article 21, alinéa 1 LPJA avant qu'une décision ne soit éventuellement rendue. L'autorité de protection des données fixe un délai raisonnable à cet égard. Le pouvoir décisionnel de l'autorité est caduc.

Article 47 – Mesures administratives

Alinéa 1

En vertu de l'article 47, paragraphe 2, lettres *b* et *c* de la directive (UE) 2016/680 et de l'article 19 STE n° 108+ concernant la modification de l'article 15, chiffre 2, lettre *c* STE n° 108, l'autorité de protection des données doit pouvoir rendre des décisions contraignantes en cas de violations du droit de la protection des données. Il faut inclure cette possibilité dans le droit cantonal. La décision pourrait par exemple exiger qu'un traitement de données illicite soit suspendu ou qu'il y soit renoncé. La compétence décisionnelle doit toutefois se limiter aux cas portant gravement atteinte aux dispositions en matière de protection des données.

Par souci d'exhaustivité, il convient ici de mentionner que les personnes concernées qui souhaitent s'opposer au traitement de leurs données par les autorités ont la possibilité de le faire en attaquant directement leurs actions. Elles peuvent utiliser les voies de droit normales à cet effet. L'autorité de protection des données ne prend alors pas part à la procédure. Exceptionnellement, l'autorité de protection des données fait parvenir une prise de position sur des questions touchant à la protection des données lorsque des instances de décision ou de recours l'y invitent dans le cadre de leur collaboration.

Alinéa 2

La loi fédérale exclut complètement les tribunaux fédéraux du champ de la surveillance (art. 4, al. 2, lit. *c* LPD). Cette exception se justifie car une telle forme de surveillance serait susceptible de nuire à l'indépendance de la justice et à la séparation des pouvoirs. Par ailleurs, le Tribunal fédéral et le Tribunal administratif fédéral sont les instances de recours contre les décisions de la préposée ou du préposé. Afin de remplir les exigences européennes, chaque tribunal fédéral va mettre en place une surveillance indépendante par voie d'ordonnance[75]. La Commission administrative du Tribunal fédéral exerce la surveillance en matière de protection des données sur le Tribunal pénal fédéral, le Tribunal administratif fédéral et le Tribunal fédéral des brevets (art. 1, al. 2 et art. 3, lit. *c*^{bis} du règlement du Tribunal fédéral relatif à la surveillance du Tribunal pénal fédéral, du Tribunal administratif fédéral et du Tribunal fédéral des brevets [règlement sur la surveillance par le Tribunal fédéral, RSTF])[76]. Les tribunaux doivent lui adresser un rapport sur la protection des données (art. 6a RSTF). Elle peut procéder à des enquêtes (art. 7 RSTF) et édicter des directives (art. 10 RSTF).

Les cantons règlent la surveillance des tribunaux de manière très différente. Parfois, les tribunaux sont exclus du champ de compétence de l'autorité de protection des données et un organe spécial est institué pour leur surveillance (p. ex. dans le canton de Zurich); parfois, une limite est fixée, l'autorité de protection des données ne pouvant pas prononcer de mesure administrative à leur encontre (c'est le cas dans les cantons de Bâle-Campagne et Bâle-Ville); par-

[75] FF 2017, p. 6638
[76] RS 173.110.132

fois encore, ils sont pleinement assujettis à la surveillance de l'autorité de protection des données (comme dans le canton de Lucerne, bien qu'une question se pose quant à savoir si un tribunal peut agir contre une mesure étant donné que les décisions de l'autorité de protection des données sont attaquables autrement devant le tribunal cantonal).

L'alinéa 2 prévoit que l'autorité cantonale de protection des données peut rendre des décisions à l'encontre également des autorités judiciaires et du Ministère public dans le cadre d'application prévu par la loi cantonale sur la protection des données (voir l'art. 3, al. 4 P-LCPD). Ainsi, la compétence décisionnelle de l'autorité cantonale de protection des données est réglée de la même manière pour toutes les autorités.

Ce qui compte c'est le fait qu'une procédure soit régie par des prescriptions procédurales. Un traitement de données personnelles survenant lors d'une procédure en cours devant les autorités judiciaires ou le Ministère public ne saurait faire l'objet de la surveillance de l'autorité de protection des données. Par contre, ils doivent soumettre à l'autorité de protection des données tous les traitements systématiques envisagés en vue d'un contrôle préalable. À cette occasion, les questions d'ordre général liées au traitement sont abordées, comme la manière de gérer des données sur des personnes autres que celle visée. Le projet dans son ensemble tient suffisamment compte de la séparation des pouvoirs.

Article 48 – Compétence en matière de recours

Alinéa 1

Si une autorité de protection des données de droit communal rend une décision contre une commune ou une autre collectivité de droit communal, l'instance de recours pourrait aussi bien être la préfecture compétente que l'autorité cantonale de protection des données. L'autorité cantonale de protection des données exerce la haute surveillance (art. 43, al. 2 P-LCPD). Cependant, cette dernière ne confère justement pas la compétence d'agir en lieu et place des organes soumis à la haute surveillance, d'annuler ni de modifier des décisions (voir aussi l'art. 4 LGC). L'autorité cantonale de protection des données ne saurait donc se qualifier pour connaître des recours.

Selon le droit en vigueur, les décisions des communes ou d'autres collectivités de droit communal pourraient être attaquées devant la préfecture compétente (art. 26 LCPD et art. 63, al. 1, lit. *a* LPJA). Il appartient aux préfectures d'exercer la surveillance cantonale (art. 87 LCo). Il y a lieu de maintenir cette organisation juridictionnelle aussi pour les décisions des autorités de protection des données de droit communal.

Alinéa 2

L'autorité de protection des données n'est subordonnée à aucune Direction. Elle est, à l'instar du Contrôle des finances, une unité administrative indépendante au sein de l'administration (voir le point 7.9.4). Le Tribunal administratif est l'instance de recours directe et ce, indépendamment de l'entité contre laquelle l'autorité cantonale de protection des données rend une décision (commune, autre collectivité de droit communal, y c. paroisses, ou autorité cantonale). Cette solution s'inscrit dans la droite ligne du guide de la CdC et correspond au système bernois des moyens de droit. Les décisions du Contrôle des finances sont elles aussi attaquables devant le Tribunal administratif[77]. Dans la mesure où l'autorité cantonale de protection des données a compétence décisionnelle, le modèle n'est pas modifié.

La question des recours contre les décisions de l'autorité de protection des données relevant d'une Église nationale doit aussi être réglée. Il ne s'agit pas là des paroisses en tant que collectivités de droit communal. En cette qualité, elles sont surveillées par l'autorité cantonale de protection des données. Les décisions des autorités relevant d'une Église nationale rendues en

[77] JAB 2023, p. 201. consid. 1.1

vertu du droit temporel, qu'il soit seul applicable ou en complément au droit ecclésiastique, doivent être directement attaquées devant les instances prévues par la loi sur la procédure et la juridiction administratives (art. 23 de la loi du 21 mars 2018 sur les Églises nationales bernoises [loi sur les Églises nationales][78]). Dès lors, la première instance de recours contre les décisions est le Tribunal administratif (art. 74 LPJA).

Dispositions non reprises:

L'article 47, paragraphe 2, lettre *c* de la directive (UE) 2016/680 et le guide de la CdC exigent une réglementation portant sur le prononcé de mesures provisoires. Si des intérêts dignes de protection sont visiblement menacés ou lésés, l'autorité de protection des données doit être habilitée à ordonner, à titre préventif, des mesures pour limiter ou interdire le traitement de données. Il serait toutefois superflu d'inscrire une norme explicite dans la loi cantonale sur la protection des données, puisque les dispositions de la loi sur la procédure et la juridiction administratives s'appliquent à la procédure et que l'article 27 LPJA prévoit déjà la possibilité d'ordonner des mesures provisionnelles.

Il est renoncé au contrôle de l'inopportunité par le Tribunal administratif. Lorsque les affaires sont de nature surtout technique, comme le sont les mesures prises pour la protection et la sécurité des données, les tribunaux ne sont souvent pas en mesure d'en examiner l'opportunité et doivent par conséquent se fonder sur les compétences spécialisées de l'autorité décisionnelle. Un pouvoir d'examen à l'égard du droit et des faits garantit une protection juridique suffisante.

Alinéa 3

En principe, les décisions et les décisions sur recours de l'autorité cantonale de protection des données peuvent être attaquées devant le Tribunal administratif dans un délai de 30 jours. Or, lorsqu'il est le destinataire d'une décision, cela ne saurait être possible. La loi prévoit donc ce cas en désignant alors la Cour suprême comme autorité de recours.

Article 49 – Coopération

Alinéa 1

La protection des données est influencée comme le reste par le fédéralisme suisse: la Confédération et les cantons ont chacun leur propre loi sur la protection des données, et dans le canton de Berne, quelques communes sont dotées de leur propre autorité de protection (art. 41 P-LCPD). Cela peut constituer un obstacle à la collaboration. Si, par exemple, une plateforme intercantonale qui doit également être utilisée par les communes est contrôlée par des dizaines d'autorités de protection distinctes sur la base de critères distincts et dans le cadre de processus distincts, les différences et les procédures de recours susceptibles d'en découler risquent de bloquer le projet durant une longue période ou de retenir d'emblée les cantons de collaborer – sans compter le surcoût lié aux nombreux processus de contrôle parallèles.

Dans le but d'éviter autant que possible de telles frictions, l'alinéa pose le principe de la collaboration entre les autorités de protection des données elles-mêmes et entre elles et d'autres autorités de surveillance. Parmi ces dernières, on peut compter des autorités de surveillance d'autres cantons, de la Confédération ou d'autres pays, que leurs activités se concentrent sur la protection des données ou non à l'instar des préfectures ou du Contrôle des finances. Les procédures de contrôle préalable en particulier doivent être coordonnées dans le temps et sur le contenu de manière à entraver le moins possible le projet de collaboration. Les autorités de protection des données doivent avoir des échanges à ce sujet, afin de pouvoir établir dans la mesure du possible un rapport de contrôle commun ou similaire et tenir compte des vérifications faites par d'autres autorités de protection des données.

[78] RSB 410.11

Alinéa 2

Comme jusqu'à présent, il est possible pour des services de protection des données d'assumer des tâches relevant de la surveillance de la protection des données dans d'autres collectivités de droit public du canton de Berne, si un accord en ce sens a été conclu par écrit. Ainsi, l'autorité cantonale de protection des données peut donner le droit à un service de protection des données extracantonal d'accomplir des tâches de contrôle dans le canton de Berne lorsque des autorités de plusieurs cantons traitent conjointement des données personnelles ou en cas de partialité des collaboratrices et collaborateurs de l'autorité cantonale de protection des données.

Alinéa 3

L'autorité cantonale de protection des données exerce une surveillance dans le cadre du concordat intercantonal sur les jeux d'argent pour lequel aucune autre autorité de protection des données ne serait sinon responsable. D'autres exemples d'application seraient la prise en charge des opérations de vérifications (audits) ou des contrôles préalables dans des communes ou des cantons à leur demande (lit. *a*).

Seule l'autorité cantonale de protection des données est compétente pour assurer la surveillance de la protection des données portant sur des projets impliquant l'utilisation de prestations numériques cantonales (comme les services de base), y compris en ce qui concerne le traitement des données par les communes qui disposent de leur propre autorité de protection des données. Elle garantit ainsi une évaluation uniforme et efficace de la situation au niveau cantonal. En l'absence de cette compétence unique, les éventuelles divergences d'opinion entre les autorités communales de protection des données risqueraient de retarder des projets ou d'entraver l'utilisation uniforme et la sécurité des prestations numériques. Il sied de souligner que le canton n'est responsable que dans la mesure où il rend le service effectivement disponible. Pour le surplus, le traitement reste de la responsabilité de la commune. En outre, cela concerne seulement le traitement de données au moyen des prestations numériques cantonales et exclut le traitement de données effectué à l'aide d'autres prestations, par exemple avec un logiciel communal (lit. *b*).

Article 50 – Rapport et information du public

Cet article porte sur le rapport annuel qui doit être remis à l'organe électoral, de même qu'aux communes et aux autres collectivités de droit communal soumises à la surveillance au besoin, et sur l'information du public. Dans son rapport d'activité, l'autorité de protection des données doit se limiter aux faits importants pour le public. Une mention sera expressément faite à cet égard par voie d'ordonnance.

Formellement, le rapport d'activité de l'autorité cantonale de protection des données s'adresse à l'organe électoral ainsi qu'au besoin aux communes et aux autres collectivités de droit communal soumises à la surveillance.

Dans la mesure où les communes et les autres collectivités de droit communal, les Églises nationales et leurs entités régionales disposent de leur propre autorité de protection des données, elles règlent elles-mêmes les modalités du rapport (al. 2). Il n'est toutefois pas possible d'y renoncer.

L'autorité cantonale de protection des données publie aujourd'hui déjà sur Internet son rapport d'activité. La publication du rapport découle de l'obligation qu'a l'autorité de protection d'informer régulièrement le public (art. 42, al. 1, lit. *i* P-LCPD) et de la législation sur l'information, de sorte qu'il n'est pas nécessaire de prévoir une règle explicite à cet égard.

Au besoin, l'autorité de protection des données peut informer le public. L'obligation qui lui était faite d'en aviser au préalable la directrice, le directeur, la chancelière ou le chancelier a volontairement été laissée de côté. L'indépendance de l'autorité de protection des données est ainsi

prise en considération. Pour le reste, un échange a lieu entre les autorités et l'autorité de protection des données selon les articles 44 à 46 P-LCPD ou dans le cadre d'une coopération informelle. En cas d'incidents d'intérêt public, une telle procédure est privilégiée. Elle permet à l'autorité concernée de s'exprimer sur les recommandations de l'autorité de protection des données, le droit d'être entendue étant ainsi garanti.

7.6 Procédure et protection juridique

Article 51 – Dispositions applicables

Le principe inscrit dans cet article signifie que la voie de recours ordinaire vaut aussi en droit de la protection des données. Ainsi, l'autorité de recours n'est pas, comme jusqu'à présent, l'autorité de protection des données. Une exception à la voie de recours ordinaire est prévue pour les cas de durcissement graduel de la situation entre les autorités et l'autorité de protection des données lorsque cette dernière statue par voie de décision. Si cette situation se présente, l'autorité cantonale de protection des données, le Tribunal administratif ou la Cour suprême sont compétents (voir l'art. 48 P-LCPD).

Article 52 – Représentation en justice

Sauf dans le domaine du droit des assurances sociales et sous réserve de toute disposition légale contraire, seuls les avocates et les avocats sont admis comme mandataires dans les procès du ressort des autorités de justice administrative selon l'article 15, alinéa 4 LPJA. Ces personnes doivent être autorisées à représenter des tiers en justice dans le canton de Berne selon la législation sur les avocates et les avocats.

L'article 55 de la directive (UE) 2016/680 conçoit une exception au monopole des avocates et avocats dans la représentation en justice. Cette exception a été introduite à l'article 11 OiDPD et doit à présent être reprise dans le droit ordinaire. La possibilité d'une représentation par des organisations d'utilité publique se limite au champ d'application de la directive. Par ailleurs, le siège de ces organisations doit se trouver en Suisse.

La directive prévoit une voie de recours contre une dénonciation à l'autorité de surveillance, contre une décision de l'autorité de la protection des données et contre une décision de l'autorité. Cette disposition a pour but de permettre aux personnes concernées d'être représentées par des organisations d'utilité publique lorsqu'une des voies de droit susmentionnées est introduite. Puisque la loi sur la procédure et la juridiction administratives garantit un monopole des avocates et des avocats dans les recours internes à l'administration ou devant une instance indépendante de celle-ci, l'exception doit être reprise à titre de droit spécial dans la loi cantonale sur la protection des données (voir l'art. 15, al. 4 LPJA). L'organisation ne peut avoir qualité de représentante que si elle est d'utilité publique. Cela veut dire qu'elle ne doit pas poursuivre de but lucratif. De plus, elle doit, en vertu de ses statuts, s'occuper des impératifs de la protection des données. S'agissant de l'interprétation de ce dernier point, il peut être renvoyé à la jurisprudence sur le droit de recours des associations. Par ailleurs, les statuts doivent obligatoirement prévoir la représentation de personnes dans les affaires relevant de la protection des données.

L'exception au monopole des avocates et des avocats vaut pour l'ensemble des procédures de recours internes à l'administration et des procédures devant le Tribunal administratif et les autres autorités de justice indépendantes de l'administration au sens de l'article 85 LPJA qui portent sur des affaires relevant de la protection des données, dans la mesure où le prévoit la directive. Les principales procédures concernées sont celles qui découlent des articles 28 ss P-LCPD, c'est-à-dire des décisions de l'autorité sur les demandes de renseignements et sur le fait

de différer ou de refuser la communication des informations. Une exception n'est pas nécessaire dans le cas des dénonciations à l'autorité de la protection des données compte tenu du fait qu'il n'y a pas de monopole en matière de droit de la surveillance.

Article 53 – Actes attaquables

Il n'est pas certain qu'une ordonnance formelle relative à une demande de renseignements ou à une requête en cas de traitement illicite (voir les art. 28 et 31 P-LCPD) réunisse tous les éléments d'une décision. La présente disposition vise à établir clairement que de telles ordonnances, y compris si elles prévoient un refus, une limitation ou un délai, sont elles aussi attaquables. Il en va de même pour la communication de données personnelles.

Article 54 – Recours d'autorités

Si une autorité demande à une autre autorité de lui communiquer des données personnelles et que celle-ci lui refuse le renseignement, l'autorité qui a essuyé un refus doit pouvoir se défendre lorsque, conformément à la loi cantonale sur la protection des données, elle a le droit d'obtenir cette information.

Article 55 – Émolument

Le droit d'accès est l'une des plus importantes expressions du droit fondamental à la protection des données, raison pour laquelle la communication de renseignements et l'exercice des autres droits de la personne concernée qui en découlent sont en principe gratuits. En conséquence, l'ensemble des droits qu'une personne concernée est apte à faire valoir selon le quatrième titre de la loi cantonale sur la protection des données peuvent être exercés sans être soumis à émolument. Par contre, l'autorité peut percevoir un émolument lorsque la personne exerce ses droits en faisant preuve de mauvaise foi ou en agissant à la légère. L'exception vise avant tout les demandes ayant un caractère procédurier et reprend une formulation usuelle dans le droit bernois.

L'exemption d'émoluments ne vaut que pour les prétentions à l'encontre de l'autorité responsable; elle ne concerne pas la procédure de recours. Pour les procédures de justice administrative, l'article 51 renvoie aux prescriptions procédurales applicables.

7.7 Dispositions d'exécution

Article 56 – Dispositions d'exécution

Cette disposition confère au Conseil-exécutif le pouvoir d'édicter les dispositions d'exécution nécessaires.

La sous-délégation concernant les détails techniques et de second ordre n'est plus nécessaire étant donné que les dispositions de l'ordonnance de Direction concernant la sûreté de l'information et la protection des données seront reprises dans l'ordonnance relative à la future loi sur la sécurité de l'information et la cybersécurité.

7.8 Dispositions transitoires et dispositions finales

7.8.1 Dispositions transitoires

Article 57 – Traitements en cours

La disposition transitoire concerne les traitements de données ayant déjà fait l'objet d'un contrôle préalable de la part d'une autorité de protection des données (communale ou cantonale) ou qui ont débuté sous l'ancien droit et qui perdurent après l'entrée en vigueur de la présente loi. En pareils cas, lorsque le traitement ne change pas de manière importante, les articles suivants ne s'appliquent pas:

- Article 9: Protection des données dès la conception et par défaut
- Article 18: Analyse des risques
- Article 19: Analyse d'impact relative à la protection des données personnelles
- Article 20: Contrôle préalable

Ces articles portent sur les obligations des autorités lors de la phase précédant le traitement. Elles n'ont pas à assumer ces obligations rétroactivement. Il est possible qu'un traitement ait déjà fait l'objet d'un contrôle préalable par une autorité de protection des données avant l'entrée en vigueur de la loi, mais qu'il ne se concrétise qu'après. Dans ce cas non plus, il n'y a pas besoin de procéder à un nouveau contrôle. Étant donné que tous les traitements ne sont pas soumis au contrôle préalable, l'exception doit également valoir pour d'autres traitements qui ont déjà débuté.

Article 58 – Procédures en cours

Pour garantir la sécurité juridique et le respect du principe de la bonne foi, cette disposition prescrit que les enquêtes de l'autorité de protection des données pendantes au moment de l'entrée en vigueur de la future loi cantonale sur la protection des données, ainsi que les recours contre les décisions, restent régis par l'ancien droit. Cette notion vise aussi bien les règles matérielles de protection des données que les compétences de l'autorité, ainsi que les autres normes de procédure applicables.

Article 59 – Compensation des charges

La concentration des tâches communales découlant du droit de la protection des données va de pair avec l'édiction de règles pour la nouvelle répartition des charges. Les autorités de protection des données qui étaient dirigées ou mandatées par les communes sont vouées pour la plupart à disparaître au profit d'une centralisation cantonale, dont résulte également un besoin en financement. L'augmentation des charges financières du canton de Berne due à la reprise du mandat de surveillance de droit communal a été calculé comme suit.

Actuellement, l'article 33a, alinéa 5 LCPD prévoit que les autorités de protection des données de droit communal ainsi que des Églises nationales et de leurs entités régionales doivent disposer de compétences propres suffisantes en matière d'autorisation de dépenses. Cette disposition est concrétisée par l'article 14 de l'ordonnance sur la protection des données en vigueur dans le canton, selon lequel les autorités de surveillance en question disposent annuellement, selon la taille de la collectivité, de la compétence en matière d'autorisation de dépenses suivante:

- Petites collectivités[79]: 1000 francs
- Autres collectivités: 5000 francs
- Communes de plus de 10 000 habitantes et habitants: 10 000 francs

Sur la base du nombre de communes, d'autres collectivités de droit communal et de petites collectivités à fin 2021 et des compétences de chacune des catégories, le calcul donne le résultat suivant:

- 530 petites collectivités: 530 000 francs
- 335 communes politiques (déduction faite des communes de 25 000 habitantes et habitants): 1 740 000 francs
- 243 paroisses: 1 215 000 francs

La charge supplémentaire qui incombe au canton de Berne ne correspond cependant pas aux montants calculés sur la base de l'article 14 OPD, dont le total se porterait à quelque 3,5 millions de francs. Dans de nombreuses communes et autres collectivités de droit communal, la surveillance de la protection des données est assumée par un organe de révision externe ou, dans les communes de grande taille, par des commissions parlementaires (commission de gestion, commission de surveillance). En règle générale, la charge réelle ne correspond pas à celle prévue conformément à l'ordonnance cantonale sur la protection des données. Dans les petites et moyennes communes et dans les autres collectivités de droit communal, la charge devrait être inférieure à 1000 francs par an. Par ailleurs, l'autorité cantonale de protection des données peut profiter des synergies créées par la concentration des connaissances (existantes et nouvelles). Cependant, la surveillance cantonale implique un renforcement des ressources en raison de la charge de travail supplémentaire. Au 31 décembre 2021, l'autorité cantonale de protection des données disposait de 570 % de postes à plein temps. Selon le rapport de gestion de 2021, les frais de personnel s'élevaient durant cet exercice à 1 067 775 francs et les charges de biens et services et autres charges d'exploitation se portaient à 174 048 francs (rectificatif selon le rapport d'activité de 2021 du Bureau pour la surveillance de la protection des données: 243 000 francs). L'autorité cantonale de protection des données prévoit des charges supplémentaires de l'ordre de quelque 400 % de poste. La centralisation des tâches ne doit pas se traduire par une situation où le canton est tenu d'assumer ces coûts supplémentaires sans compensation. Le montant total des frais de personnel supplémentaires et des dépenses d'exploitation accrues, estimé à un million de francs environ, doit être pris en compte dans le système de compensation des charges.

Le transfert de charges entre les communes et le canton résultant de la centralisation des tâches relevant de la protection des données sera imputé au titre de la compensation des charges, dès l'entrée en vigueur de la présente loi, conformément à l'article 29b de la loi du 27 novembre 2000 sur la péréquation financière et la compensation des charges (LPFC)[80].

Le système de l'article 29b LPFC a créé un instrument permettant de compenser des transferts de charges entre le canton et les communes dans le cas d'une nouvelle répartition des tâches[81]. Cet instrument offre justement une solution adéquate pour les transferts de charges dans la mesure présentement considérée. Ces derniers doivent par conséquent être supportés par l'ensemble des communes. Exclure quelques communes de la compensation des charges selon l'article 29b LPFC est incompatible avec la disposition et n'est pas possible. Le transfert de charges doit donc être supporté par toutes les communes.

[79] Sections de commune, communes et corporations bourgeoises, syndicats de communes et corporations de digues (art. 64a de l'ordonnance du 16 décembre 1998 sur les communes [OCo; RSB 170.111])
[80] RSB 631.1
[81] Lienhard, Andreas; Engel Gerhard; Schmutz Andreas (2021). Finanzrecht. in: Müller, Markus; Feller, Reto (éd.), Kommentar zum bernischen Verwaltungsrecht. Berne: éditions Stämpfli SA, p. 1002

Article 60 – Période de fonction de la déléguée ou du délégué à la protection des données

La disposition transitoire porte notamment sur les préparatifs de l'élection de la déléguée ou du délégué à la protection des données et sur la durée de son mandat. La période de fonction doit coïncider avec la législature. C'est ainsi que le Grand Conseil élit la chancelière ou le chancelier lors de sa séance constitutive. La disposition transitoire souligne le fait que la déléguée ou le délégué à la protection des données, une fois l'élection passée, conserve son mandat pour toute la période de fonction. Dans le cas de la première élection ou réélection suivant l'entrée en vigueur de la loi, la période de fonction est raccourcie de neuf mois, car la personne n'est élue que pour la durée de la législature en cours.

Il devient donc nécessaire de modifier le règlement du Grand Conseil. Un acte législatif de rang inférieur ne peut pas faire l'objet d'une modification indirecte (parallélisme des formes). La modification du règlement constitue pour cette raison un projet à part. L'élection de la déléguée ou du délégué à la protection des données requiert l'ajout de la lettre *m1* à l'article 1 RGC (élection lors de la séance constitutive du Grand Conseil) et de la lettre *f* à l'article 109, alinéa 1 RGC (chronologie).

Article 61 – Évaluation

Pour pouvoir s'assurer que la loi est appliquée efficacement, il s'agit de l'évaluer. L'évaluation prendra la forme d'un rapport, rédigé quatre ans après l'entrée en vigueur de la loi par le Conseil-exécutif à l'intention du Grand Conseil.

7.9 Modifications d'autres actes législatifs

7.9.1 Loi du 19 février 1986 sur la protection des données (LCPD)[82]

La loi sur la protection des données étant soumise à une révision totale, le texte législatif actuellement en vigueur doit être abrogé.

7.9.2 Modification indirecte de la loi du 7 mars 2022 sur l'administration numérique (LAN)[83]

Les dispositions concernant le traitement de données par des tiers (art. 28 LAN), la responsabilité en matière de protection des données lors du traitement commun de données personnelles par plusieurs autorités (art. 29 LAN) et la surveillance de la protection des données dans la collaboration entre autorités (art. 30 LAN) sont introduites sous une forme légèrement adaptée dans la loi cantonale sur la protection des données (art. 12 et art. 49 P-LCPD). Le chapitre 5 de la loi sur l'administration numérique peut donc être entièrement supprimé. Un renvoi à la loi cantonale sur la protection des données n'est pas nécessaire puisque, même s'il n'y en a pas, les dispositions qui se trouvent dans la loi valent pour l'ensemble des traitements de données personnelles.

[82] RSB 152.04
[83] RSB 109.1

7.9.3 Modification indirecte de la loi du 12 septembre 1985 sur l'établissement et le séjour des Suissesses et des Suisses (LES)[84] et de la loi du 9 décembre 2019 portant introduction de la loi fédérale sur l'asile et de la loi fédérale sur les étrangers et l'intégration (Li LFAE)[85]

La révision synthétise les dispositions relatives aux communications de données personnelles et la règle liée à leur communication par les communes municipales est déplacée dans des lois spéciales. Cette règle entre dans le domaine matériel du droit de la protection des données. Elle ne doit donc pas figurer dans un texte à portée transversale et n'était pas à sa place dans la loi actuellement en vigueur.

La version modifiée de l'article 12 ne doit plus que porter sur la communication à des personnes privées. La communication aux autorités est régie par les principes généraux de la loi cantonale sur la protection des données, et par l'article 14 P-LCPD en particulier.

Conformément à l'énumération de l'alinéa 1, le contrôle des habitantes et des habitants indique désormais le nouveau domicile, en plus des dates d'arrivée et de départ, ce qui correspond aux habitudes des communes. Pour le reste, les renseignements sont ceux fixés à l'actuel article 12, alinéa 1 LCPD.

En dérogation à l'article 33 P-LCPD, la personne concernée peut demander le blocage de la communication de données supplémentaires, qui serait admissible au vu du règlement communal, sans prouver qu'elle y trouve un intérêt digne de protection.

Le renvoi aux prescriptions sur la protection des données de l'article 12, alinéa 1 LES doit être supprimé à l'occasion de l'introduction de la règlementation spéciale.

La disposition doit aussi s'appliquer à la communication de données personnelles des ressortissantes étrangères et des ressortissants étrangers. Il y a donc lieu d'inscrire un renvoi à la loi sur l'établissement et le séjour des Suissesses et des Suisses dans la loi portant introduction de la loi fédérale sur l'asile et de la loi fédérale sur les étrangers et l'intégration.

7.9.4 Modification indirecte de la loi du 20 juin 1995 sur l'organisation du Conseil-exécutif et de l'administration (loi d'organisation, LOCA)[86]

La révision a été l'occasion de s'interroger sur la position de l'autorité cantonale de protection des données au niveau organisationnel. Son statut est comparable à celui du Contrôle des finances: les deux unités administratives sont indépendantes sur les plans organisationnel et institutionnel. Elles sont seulement soumises à la Constitution et à la loi. Leur rattachement à l'administration est purement administratif, la personne qui les dirige est élue par le Grand Conseil et a le statut, conformément au droit du personnel, d'un membre d'autorité à titre principal. L'autorité est en outre placée sous la surveillance du Grand Conseil et tient une comptabilité séparée. Pour les questions de fond ainsi qu'en matière d'organisation, de personnel et de finances, elle n'est donc pas liée par des instructions, ce qui lui confère un statut indépendant de l'administration. Cela pourrait porter à croire que le statut qui lui est accordé la place hors de l'administration, à l'image des tribunaux. Comme déjà constaté à juste titre dans le rapport accompagnant la modification de 2008 de la loi sur la protection des données, l'indépendance de l'autorité cantonale de protection des données ne doit pas conduire à une situation qui verrait cet organe se transformer en un «quatrième pouvoir» incontrôlé voire à un «État dans l'État». Par conséquent, l'autorité cantonale de protection des données doit être rattachée à l'un des trois pouvoirs (législatif, exécutif et judiciaire), et l'exécutif est le seul à entrer raisonnablement

[84] RSB 122.11
[85] RSB 122.20
[86] RSB 152.01

en ligne de compte. De ce fait, l'autorité cantonale de protection des données peut être considérée comme une unité administrative indépendante. Elle n'évolue donc pas hors de l'administration, mais est une composante autonome de l'administration.

En harmonisation avec la solution retenue pour le Contrôle des finances, le titre 2a doit être complété de la mention «autorité cantonale de protection des données» et un article supplémentaire (art. 40b) doit être créé par analogie à celui du Contrôle des finances, qui désigne l'autorité cantonale de protection des données comme une unité administrative indépendante. Il ressort en outre de la systématique que l'autorité cantonale de protection des données appartient à l'administration.

7.9.5 Modification indirecte de la loi du 10 février 2019 sur la police (LPol)[87]

En conformité avec le droit supérieur, la personne responsable de la protection des données selon l'article 150, alinéa 1 LPol doit dorénavant s'appeler une conseillère ou un conseiller à la protection des données.

Par ailleurs, le renvoi de l'article 141 LPol concernant la législation cantonale sur la protection des données doit être adapté.

7.9.6 Modification indirecte de la loi du 9 mars 2021 sur les programmes d'action sociale (LPASoc)[88] et de la loi cantonale du 10 juin 2020 sur les jeux d'argent (LCJar)[89]

Le droit en vigueur ne nomme que des mesures d'assistance comme données personnelles sensibles; or telles que comprises aujourd'hui, elles devraient en principe aussi englober les mesures de protection de l'enfant et de l'adulte[90]. Ces données comprennent par exemple celles qui se rapportent à des placements à des fins d'assistance. Dans la législation bernoise, la terminologie est déjà partiellement modifiée. C'est le cas notamment à l'article 57d, alinéa 4 de la loi du 11 juin 2001 sur l'aide sociale (LASoc)[91]. La révision doit servir à passer de l'expression «mesures d'assistance» à «mesures de protection de l'enfant et de l'adulte» dans les articles 71 LCJar[92] et 111, alinéa 2 LPASoc[93] (voir l'art. 2, al. 1, ch. 6 P-LCPD).

7.9.7 Adaptations liées au nouveau titre de l'acte (modifications indirectes)

Les lois suivantes renvoient de manière générale à la loi sur la protection des données ou de manière spécifique à ses dispositions. La modification du titre de l'acte législatif entraîne celle des renvois. Dans la mesure du possible, il convient de renvoyer au texte et de manière dynamique, sans référence à des articles concrets. Des modifications de loi ultérieures s'en trouvent ainsi simplifiées. Les modifications indirectes suivantes sont nécessaires:

- Article 29 de la loi du 2 novembre 1993 sur l'information et l'aide aux médias (LIAM)[94]
- Article 9a, article 14 et article 20 de la loi du 31 mars 2009 sur l'archivage (LArch)[95]

[87] RSB 555.1
[88] RSB 860.2
[89] RSB 935.52
[90] Voir Rudin, Beat (2014), *op. cit.,* n. 38 ad § 3
[91] RSB 860.1
[92] RSB 935.52
[93] RSB 860.2
[94] RSB 107.1
[95] RSB 108.1

- Article 2, article 4, article 7, article 11, article 13, article 15 et article A1-1 de la loi du 10 mars 2020 sur les fichiers centralisés de données personnelles (LFDP)[96]
- Article 12a de la loi du 16 septembre 2004 sur le personnel (LPers)[97]
- Article 35 de la loi du 18 mai 2014 sur les caisses de pension cantonales (LCPC)[98]
- Article 23 de la loi du 23 mai 1989 sur la procédure et la juridiction administratives (LPJA)[99]
- Article 55 de la loi du 1er février 2012 sur la protection de l'enfant et de l'adulte (LPEA)[100]
- Article 3 de la loi du 11 juin 2009 portant introduction du code de procédure civile, du code de procédure pénale et de la loi sur la procédure pénale applicable aux mineurs (LiCPM)[101]
- Article 38 de la loi cantonale du 7 mars 2022 sur le Contrôle des finances (LCCF)[102]
- Article 130 de la loi du 13 juin 2013 sur les soins hospitaliers (LSH)[103]
- Article 57g et article 80g de la loi du 11 juin 2001 sur l'aide sociale (LASoc)[104]
- Article 46 et article 51 de la loi du 3 décembre 2019 sur l'aide sociale dans le domaine de l'asile et des réfugiés (LAAR)[105]
- Article 71 de la loi cantonale du 10 juin 2020 sur les jeux d'argent (LCJAr)[106]

Il convient de se référer aux points 7.9.1 à 7.9.6 pour les modifications indirectes de la loi sur l'administration numérique, de la loi sur l'établissement et le séjour des Suissesses et des Suisses, de la loi portant introduction de la loi fédérale sur l'asile et de la loi fédérale sur les étrangers et l'intégration, de la loi d'organisation, de la loi sur la police, de la loi sur les programmes d'action sociale et de la loi cantonale sur les jeux d'argent.

7.9.8 Adaptation de la terminologie française concernant les données sensibles (modifications indirectes)

L'occasion de la révision permet une adaptation terminologique. Les données particulièrement dignes de protection seront désignées sous le nom de «données personnelles sensibles (données sensibles)». Cette adaptation est à l'origine de plusieurs modifications indirectes:

- Articles 28 et 29 de la loi du 2 novembre 1993 sur l'information et l'aide aux médias (LIAM)[107]
- Article 31 de la loi du 7 mars 2022 sur l'administration numérique (LAN)[108]
- Article 25 de la loi du 13 juin 2017 sur le droit de cité cantonal et le droit de cité communal (loi sur le droit de cité, LDC)[109]
- Articles 37 et 38 de la loi du 9 décembre 2019 portant introduction de la loi fédérale sur l'asile et de la loi fédérale sur les étrangers et l'intégration (Li LFAE)[110]
- Articles 4, 5, 7, 18 et 24 de la loi du 10 mars 2020 sur les fichiers centralisés de données personnelles (LFDP)[111]
- Article 11a de la loi du 28 mars 2006 sur les préfets et les préfètes (LPr)[112]

[96] RSB 152.05
[97] RSB 153.01
[98] RSB 153.41
[99] RSB 155.21
[100] RSB 213.316
[101] RSB 271.1
[102] RSB 622.1
[103] RSB 812.11
[104] RSB 860.1
[105] RSB 861.1
[106] RSB 935.52
[107] RSB 107.1
[108] RSB 109.1
[109] RSB 121.1
[110] RSB 122.20
[111] RSB 152.05
[112] RSB 152.321

- Articles 12a, 12f et 12g de la loi du 16 septembre 2004 sur le personnel (LPers)[113]
- Article 20a de la loi du 22 novembre 2005 sur le notariat (LN)[114]
- Articles 38 et 39 de la loi du 3 décembre 2020 sur les prestations particulières d'encouragement et de protection destinées aux enfants (LPEP)[115]
- Articles 23, 24, 25 et 26 de la loi du 23 janvier 2018 sur l'exécution judiciaire (LEJ)[116]
- Articles 19 et 21 de la loi du 21 mars 2018 sur les Églises nationales bernoises (loi sur les Églises nationales, LEgN)[117]
- Articles 6 et 7 de la loi du 28 janvier 1997 concernant les communautés israélites[118]
- Articles 21d et 73 de la loi du 19 mars 1992 sur l'école obligatoire (LEO)[119]
- Article 67 de la loi du 27 mars 2007 sur les écoles moyennes (LEM)[120]
- Article 57a de la loi du 14 juin 2005 sur la formation professionnelle, la formation continue et l'orientation professionnelle (LFOP)[121]
- Article 24 de la loi cantonale du 7 décembre 2021 sur l'encouragement du sport (LCESp)[122]
- Articles 66, 141, 144, 145, 146, 148 et 160 de la loi du 10 février 2019 sur la police (LPol)[123]
- Article 14 de la loi du 13 juin 2018 sur les prestations des entreprises de sécurité privées (LPESP)[124]
- Article 66 de la loi du 15 juin 2022 sur les finances (LFin)[125]
- Article 28 de la loi cantonale du 7 mars 2022 sur le Contrôle des finances (LCCF)[126]
- Article 34a de la loi du 9 juin 1985 sur les constructions (LC)[127]
- Article 17b1 de la loi du 2 décembre 1984 sur la santé publique (LSP)[128]
- Article 4 de la loi du 6 septembre 2018 portant introduction de la législation fédérale sur l'enregistrement des maladies oncologiques (LiLEMO)[129]
- Article 14 de la loi du 23 juin 2003 sur le marché du travail (LMT)[130]
- Articles 4 et 21a de la loi du 6 juin 2000 portant introduction des lois fédérales sur l'assurance-maladie, sur l'assurance-accidents et sur l'assurance militaire (LiLAMAM)[131]
- Article 57e de la loi du 11 juin 2001 sur l'aide sociale (LASoc)[132]
- Articles 56, 102 et 111 de la loi du 9 mars 2021 sur les programmes d'action sociale (LPASoc)[133]
- Articles 46, 47 et 49 de la loi du 13 juin 2023 sur les prestations de soutien aux personnes en situation de handicap (LPHand)[134]
- Articles 45, 46, 47 et 48 de la loi du 3 décembre 2019 sur l'aide sociale dans le domaine de l'asile et des réfugiés (LAAR)[135]
- Article 44a de la loi cantonale du 16 juin 1997 sur l'agriculture (LCAB)[136]
- Articles 71 et 72 de la loi cantonale du 10 juin 2020 sur les jeux d'argent (LCJAr)[137]

[113] RSB 153.01
[114] RSB 169.11
[115] RSB 213.319
[116] RSB 341.1
[117] RSB 410.11
[118] RSB 410.51
[119] RSB 432.210
[120] RSB 433.12
[121] RSB 435.11
[122] RSB 437.11
[123] RSB 551.1
[124] RSB 551.4
[125] RSB 620.0
[126] RSB 622.1
[127] RSB 721.0
[128] RSB 811.01
[129] RSB 815.21
[130] RSB 836.11
[131] RSB 842.11
[132] RSB 860.1
[133] RSB 860.2
[134] RSB 860.3
[135] RSB 861.1
[136] RSB 910.1
[137] RSB 935.52

- Articles 21 et 23 de la loi du 7 juin 2012 sur l'exercice de la prostitution (LEP)[138]

8. Place du projet dans le programme gouvernemental de législature (programme législatif) et dans d'autres planifications importantes

La révision correspond à l'objectif stratégique nº 2 du programme gouvernemental de législature, selon lequel le canton de Berne exploite les opportunités de la transition numérique pour fournir des services efficaces, de haute qualité et efficients. Le projet de loi contribue à cet objectif par le transfert à l'autorité cantonale de protection des données des tâches qui incombaient aux autorités communales compétentes dans le domaine (et qui incomberont encore aux quatre communes les plus peuplées). Les communes se trouveront déchargées des défis actuels et prochains que présente le monde numérique et la surveillance ne sera plus qu'exercée par des professionnelles et des professionnels. Le savoir-faire ainsi concentré garantira non seulement une meilleure efficience, mais donnera aussi aux autorités communales ainsi qu'à la population accès à un service professionnel.

9. Répercussions financières

Les adaptations obligatoires au droit supérieur des dispositions ont des répercussions financières. Des moyens supplémentaires devront être mis en œuvre en particulier parce que l'autorité de protection des données aura la possibilité de rendre des décisions et la surveillance relevant du droit communal sera pour la plus grande partie centralisée et assumée par le canton. Les charges supplémentaires du canton sont toutefois remboursées par la compensation des charges (voir le commentaire de l'art. 59 P-LCPD).

L'analyse d'impact relative à la protection des données personnelles nouvellement introduite correspond pour la plus grande part aux instruments actuels, c'est-à-dire l'analyse SIPD et le concept SIPD, de sorte qu'elle n'engendre en principe aucune augmentation significative des frais. Certes, les autorités, qui n'étaient jusque-là soumises à aucune obligation en la matière, doivent procéder à cette analyse, mais, en fin de compte, leur charge de travail ne s'en trouvera pas accrue. Elles doivent en effet déjà se soumettre à un contrôle préalable et évaluer les risques d'un traitement des données. Le fait de formaliser l'analyse des risques et l'analyse d'impact relative à la protection des données personnelles n'a qu'une conséquence: la procédure est standardisée et ancrée dans la loi.

Les nouvelles obligations en matière d'information et d'annonce peuvent certes imposer un supplément de charges aux autorités, mais les coûts devraient rester dans la limite des moyens disponibles. Par ailleurs, il revient aux autorités d'empêcher tout incident en prenant les mesures techniques et organisationnelles appropriées.

10. Répercussions sur le personnel et l'organisation

En raison de la centralisation de la surveillance qui relève du droit communal, l'autorité cantonale de protection des données a besoin de 400 % de poste supplémentaires. Le surcoût est pris en compte par le système de compensation des charges (commentaire de l'art. 59 P-LCPD).

[138] RSB 935.90

11. Répercussions sur les communes

Le projet implique une diminution de charge pour les communes – sauf pour les quatre communes les plus peuplées – en raison de la centralisation des tâches relevant de la protection des données au sein de l'autorité cantonale. Elles supportent le surcoût que le changement représente pour le canton par le système de compensation des charges. Elles devraient cependant payer un prix bien moindre par rapport à celui d'aujourd'hui.

12. Répercussions sur l'économie

La loi cantonale sur la protection des données ne s'adresse directement qu'aux autorités du canton de Berne. La loi ne s'applique qu'indirectement aux tiers, en particulier les entreprises, lorsqu'ils agissent sur mandat du canton. Dans un tel cas, les tiers mandatés ne peuvent traiter des données personnelles autrement que dans la mesure où le ferait l'autorité. Ils doivent ainsi également se conformer aux dispositions relatives à la protection des données.

L'analyse effectuée sur la base de la check-list pour l'analyse d'impact de la réglementation a montré que le projet n'a dans l'ensemble pas de répercussions notables sur la charge administrative et financière des entreprises ou sur l'économie.

13. Résultat de la procédure de consultation

Le 21 juin 2023, le Conseil-exécutif a habilité la Direction de l'intérieur et de la justice à lancer une procédure de consultation relative à la révision totale de la loi cantonale sur la protection des données. La procédure a duré du 23 juin 2023 au 29 septembre 2023. Les 65 participantes et participants ont envoyé des prises de position parfois très détaillées; toutes se concentraient avant tout sur quelques sujets clés.

13.1 Champ d'application pour les personnes morales

Lors de la procédure de consultation, des opinions différentes ont été formulées quant au maintien des personnes morales dans le champ d'application de la loi cantonale sur la protection des données. Le groupe d'intérêt IG ländlicher Raum, l'UDC, la ville de Thoune et le Parti pirate étaient en faveur du maintien, tandis que le Groupe de l'Île et l'Association des avocats bernois (AAB), notamment, s'y opposaient. Ces derniers renvoient au législateur fédéral, qui limite la protection au sens de sa loi aux personnes physiques et indique ce qui suit dans son message[139]:

«En ce qui concerne le secteur public, l'abrogation de la protection des données des personnes morales a pour conséquence que les bases légales prévues par le droit fédéral qui habilitent les organes fédéraux à traiter des données personnelles ne s'appliquent plus lorsque ceux-ci traitent des données concernant des personnes morales. Or l'article 5 Cst. exige que l'activité de l'État soit régie par la loi. De plus, les personnes morales bénéficient de la protection de la sphère privée, bien qu'elles ne soient pas titulaires de tous les aspects protégés par l'article 13 Cst. Le Conseil fédéral propose par conséquent de créer une série de dispositions légales dans la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA), qui règlent la marche à suivre concernant les traitements de données concernant des personnes morales par les organes fédéraux (cf. ch. 9.2.8). Par ailleurs, une disposition transitoire permet

[139] FF 2017, p. 6595

d'éviter l'apparition de lacunes juridiques pendant cinq ans (art. 66 P-LPD et les explications sous ch. 9.1.11).»

Contrairement au projet cantonal, la loi fédérale vaut également pour les personnes privées qui traitent des données personnelles. Pour les cas où des organes fédéraux traitent les données de personnes morales, le législateur fédéral crée des **dispositions de protection des données parallèles**. Les personnes privées qui se voient déléguer une tâche par la Confédération sont considérées comme des organes fédéraux.

Créer une législation parallèle n'a guère de sens. La démarche s'accompagne aussi de difficultés pratiques. Le droit cantonal ne connaît pas d'acte applicable à l'ensemble des autorités: la loi d'organisation, par exemple, ne concerne pas les communes et la loi sur les communes ne vaut pas pour certaines institutions ecclésiales. Quant aux personnes privées qui assument des tâches publiques, il n'existe pas non plus d'acte unique. Ainsi, les dispositions sur la protection des données des personnes morales se trouveraient disséminées dans plusieurs actes législatifs. Il faut toutefois reconnaître qu'il manquait, dans le projet soumis, une **définition** de ce que sont les **données sensibles des personnes morales**. Le manque est désormais comblé, puisque la notion est définie à l'article 2, alinéa 1, lettre *d* P-LCPD selon les termes du législateur fédéral. De plus, quelques **exceptions au champ d'application** sont prévues dans la mesure où les dispositions de la protection des données ne découlent pas automatiquement de la Constitution bernoise. Il convient ici d'indiquer que la Constitution va relativement loin. L'énoncé de l'article 18 ConstC, en plus de prévoir les droits de la personne concernée (al. 1), conditionne, par l'alinéa 2, tout traitement de données personnelles à l'existence d'une base légale ainsi qu'à la nécessité et l'adéquation du traitement (= proportionnalité) pour l'accomplissement des tâches (= finalité déterminée). En outre, le constituant oblige les autorités à s'assurer que les données traitées sont exactes et à les protéger contre un emploi abusif (al. 3). Par ailleurs, de l'avis du législateur fédéral, les personnes morales peuvent se prévaloir des droits des personnes concernées même si la loi sur l'organisation du gouvernement et de l'administration ne le prévoit pas explicitement[140]. Cela signifie que les principes fixés à la section 2 LCPD valent de par la Constitution cantonale. Les droits des personnes concernées listés à la section 4 sont également applicables. Des exceptions sont possibles en vertu de la section 3 (obligations des autorités et des tiers mandatés) et de la section 5 (autorité de protection des données). Par conséquent, ces sections sont exclues du champ d'application pour les données personnelles des personnes morales.

13.2 Définitions

Par rapport au projet soumis à la procédure de consultation, la loi ne parle plus d'«autorités responsables», mais simplement d'«autorités». Du point de vue du contenu, l'article 11 continue de régler qui est responsable de la protection des données. Une uniformisation a aussi eu lieu en allemand dans l'utilisation des mots désignant le traitement et l'acquisition (forme substantive conservée; forme verbale remplacée).

Plusieurs prises de position déposées lors de la procédure de consultation demandaient que les dispositions concernant les définitions **se rapprochent** davantage de celles retenues par la **Confédération**. Cette demande est mise en œuvre dans la mesure où elle est pertinente (voir le commentaire de l'art. 2 P-LCPD pour les termes). Pour les termes qui ne sont pas modifiés, une explication est fournie ci-après.

S'agissant des mesures d'aide sociale, le projet législatif doit s'adosser à la législation cantonale. Les mesures d'aide sociale dans le canton de Berne ne correspondent pas à la même notion au niveau fédéral.

[140] FF 2017, p. 6734

Le législateur renonce volontairement à la notion d'«appartenance à une race», puisqu'elle n'est plus d'actualité. La notion de données sur l'origine ethnique reste normée dans un chiffre à part, puisqu'elle n'a rien de commun avec les notions de santé et de sphère intime.

La définition simplifiée du profilage est maintenue afin que le texte reste compréhensible. De plus, seul le profilage à risque élevé est déterminant pour les autorités cantonales.

Le terme d'autorités recouvre nécessairement une autre réalité, puisque la loi n'est pas applicable aux mêmes autorités.

La violation de la sécurité des données n'est plus normée dans les définitions mais est réglée dans le droit matériel (art. 25, al. 2 P-LCPD).

13.3 Base juridique pour le traitement des données personnelles

La base juridique a donné lieu à de nombreuses exigences très différentes, parfois contradictoires. Le PLR a demandé que tous les traitements soient conditionnés par une base au niveau de la loi. La ville de Berne, entre autres, était en faveur du maintien de la réglementation actuelle. Les Juristes démocrates de Berne et les VERT-E-S ont souhaité que les exigences formulées à l'article 18, alinéa 2 ConstC (traitement nécessaire et adéquat à l'accomplissement de tâches) soient déjà fixées dans le cadre de la base juridique. L'ACB et la ville de Thoune étaient d'avis, au contraire, qu'une base légale indirecte devait suffire lorsque le traitement sert à l'accomplissement d'une tâche légale au motif que la formulation choisie augmentait les exigences.

La loi cantonale sur la protection des données prend sa source dans la Constitution. Tout traitement de données personnelles par des autorités constitue une **atteinte** aux droits fondamentaux des personnes concernées. Conséquence du principe de la légalité fixé par le droit constitutionnel (art. 5, al. 1 et art. 36, al. 1 Cst., art. 28 ConstC), le traitement de données personnelles exige aussi une base légale. La teneur de l'article 18, alinéa 2 ConstC est la suivante:

Les autorités ne peuvent traiter des données personnelles que s'il existe une ***base légale*** (= base juridique) *et pour autant que ces données* ***sont nécessaires et adéquates à l'accomplissement de leurs tâches*** (= proportionnalité).

Les restrictions graves d'un droit fondamental doivent être prévues dans la loi. La loi cantonale sur la protection des données définissait de manières diverses, parfois fausses, les termes. Ainsi, l'article 5, alinéa 1 LCPD exige aujourd'hui que le traitement de données personnelles ordinaires soit aussi autorisé par une base fixée **dans la loi**. L'article constitutionnel susmentionné s'en trouve contredit et le droit en vigueur doit donc être révisé.

Voici le **principe**: en fonction de la gravité de l'atteinte portée aux droits fondamentaux, le traitement exige une base dans la loi ou dans un autre instrument juridique. Le **législateur exprime ainsi un jugement de valeur**. Selon ce principe, le traitement de données sensibles constitue une atteinte grave et suppose une base dans la loi (voir l'art. 4, al. 2 P-LCPD et art. 34, al. 2 LPD). Cette base peut être **directe ou indirecte**. Elle est directe lorsque le traitement est une conséquence directe, tandis qu'elle est indirecte lorsque le traitement découle de l'accomplissement d'une tâche. Pour autant qu'une autorité traite des données personnelles, elle doit en outre veiller au principe de la proportionnalité. La proportionnalité est toutefois réglée dans l'article 7 P-LCPD plutôt que dans la base juridique. Aussi la proposition de la ville de Thoune et de l'ACB a-t-elle été retenue: il suffit que le traitement serve à l'accomplissement d'une tâche légale, comme jusqu'à présent. Cependant, le traitement doit rester nécessaire et adéquat à l'accomplissement de la tâche, tout en étant acceptable pour la personne concernée (= principe de la proportionnalité).

Jugeant la différence trop floue, le Groupe de l'Île et les Services psychiatriques universitaires (SPU) ont demandé de renoncer aux différentes exigences au niveau de la loi pour le **profilage**. Par rapport au projet soumis à la consultation, la notion de profilage a été redéfinie sur la base de la notion de profilage à risque élevé de la Confédération. Pour ce type de profilage, une base inscrite dans la loi est toujours nécessaire. Cependant, étant donné que l'autorité traite des données personnelles à chaque fois qu'elle exploite un profilage, une base dans le droit matériel au moins est requise (voir l'art. 4 P-LCPD). Cela tient compte du postulat présenté au début, selon lequel tous les profilages ne représentent pas un potentiel danger. La solution retenue est toutefois nettement plus élégante que celle utilisée au niveau fédéral, qui n'a du reste été introduite qu'au moment des débats parlementaires.

La ville de Langenthal a demandé qu'un **consentement** permette de renoncer totalement à l'existence d'une base juridique. Comme le projet soumis à la consultation l'exposait déjà, le canton est d'avis que les autorités sont liées par le principe de la légalité lors du traitement de données personnelles. Le consentement ne peut donc pas libérer de l'obligation de fonder un traitement sur une base juridique. Quant au Parti pirate, il a exigé que seul le consentement de la personne concernée permette de dispenser de l'obligation eu égard à des données sensibles rendues accessibles au public. La proposition n'est pas retenue car la disposition ne doit pas s'écarter de celle de la Confédération.

Sur la base de la proposition de la ville de Thoune et de l'ACB, le projet de loi **renonce à la réserve du secret de fonction**, qui se trouvait dans l'article 5, alinéa 5 LCPD. Les agentes et les agents sont tenus de taire les faits dont ils ont eu connaissance dans l'exercice de leurs fonctions (art. 58 LPers)[141].

13.4 Communication à l'étranger: variante proposée

La CJUE a rendu l'arrêt Schrems II le 16 juillet 2020, dans lequel elle constate que les États-Unis d'Amérique n'offrent pas un niveau de protection des données personnelles équivalent à celui prévu par le droit de l'Union européenne. Cet arrêt a rendu la situation incertaine en Suisse pour ce qui est notamment des modalités d'utilisation des solutions en nuage, telles que Microsoft 365, qui permettent dans certaines circonstances la communication de données personnelles à l'étranger. Le Conseil-exécutif a donc envoyé en consultation deux variantes pour la communication de données personnelles à l'étranger. En principe, des autorités peuvent communiquer des données personnelles à l'étranger si elles garantissent un niveau de protection approprié, sauf lorsqu'elles peuvent faire valoir un cas de dérogation (variante 1). La variante 2 prévoyait une exception, à titre supplémentaire, si les conditions d'un traitement sur mandat étaient réunies, indépendamment du niveau de protection assuré. Dans l'avis de droit d'octobre 2023, Mesdames Astrid Epiney et Nula Frei sont parvenues à la conclusion que la variante 2 était aussi bien vaine qu'irrecevable selon le droit international et le droit constitutionnel.

Le contexte légal étant ce qu'il est aux États-Unis d'Amérique, un tiers mandaté peut sous certaines conditions traiter des données personnelles dans une mesure qui ne coïncide pas avec ce que l'autorité est habilitée à faire. Une analyse des risques sur la probabilité qu'un autre traitement puisse effectivement avoir lieu n'y trouve pas sa place, puisque le respect ou le non-respect du droit n'est pas une question de risque, mais une question juridique qui peut appeler une réponse différente pour les autorités étatiques et pour les personnes privées. Aucun argument juridique convaincant ne vient valider la variante 2, raison pour laquelle celle-ci est abandonnée.

Il reste à ajouter que la situation à l'égard des États-Unis d'Amérique n'est plus tout à fait la même. Les conditions offertes par le nouveau Swiss-U.S. Data Privacy Framework garantissent

[141] RSB 153.01

la sécurité des échanges de données personnelles entre la Suisse et les entreprises certifiées aux États-Unis d'Amérique selon le Conseil fédéral. Ce dernier a adapté en conséquence l'ordonnance sur la protection des données et a ajouté le pays dans cette mesure à la liste de ceux qui garantissent un niveau de protection des données adéquat. La nouvelle teneur est entrée en vigueur le 15 septembre 2024. À partir du moment et pour toute la période où des entreprises étasuniennes certifiées figurent sur la liste de l'annexe 1 de l'ordonnance sur la protection des données, la communication de données personnelles est admise dans ce cadre, conformément à l'article 15, alinéa 1, lettre *b* P-LCPD également.

13.5 Conservation, destruction et archivage

À l'issue de la procédure de consultation, il est apparu que, pour certaines parties prenantes, la différence entre le délai de conservation fixé au préalable par l'autorité et la poursuite de la conservation au-delà de ce délai à des fins de preuve ou de sécurité ou pour la recherche scientifique n'était pas claire. Voici le détail: la conservation sert de preuve que l'autorité a assumé selon les règles de l'art sa mission primaire, qu'elle a fondé son travail sur la base juridique d'origine et qu'elle l'a fait pour la finalité première. Le délai de conservation fixé par l'autorité est une application générale du principe de la proportionnalité. Une fois le délai passé, l'autorité doit détruire les données *ou* justifier pour chaque cas pourquoi elles doivent être conservées comme moyen de preuve ou de sécurité (c.-à-d. pourquoi elles restent nécessaires dans le cadre de l'accomplissement de la tâche primaire selon la base juridique initiale) ou qu'il existe une nouvelle finalité fondée sur une nouvelle base juridique (art. 17 P-LCPD concernant la recherche ou loi sur l'archivage) pour laquelle les données sont nécessaires.

13.6 Analyse des risques en cas de traitements répétés envisagés

Pour chaque traitement répété envisagé, l'autorité évalue elle-même les risques qu'il présente pour les personnes concernées (niveau 1, art. 18 P-LCPD). Si le risque est élevé, l'autorité procède à une analyse d'impact relative à la protection des données personnelles (niveau 2, art. 19 P-LCPD). Lors de la procédure de consultation, plusieurs participantes et participants (SPU, Les VERT-E-S, JDB, clinique privée Wyss) ont exigé que la disposition soit adaptée au droit fédéral et que la liste des éléments entraînant un risque élevé pour les personnes concernées ne soit pas formulée de manière exhaustive. La disposition est adaptée à cet égard au droit fédéral. La liste n'est pas exhaustive, comme le veut aussi la loi fédérale sur la protection des données. Lorsqu'un grand nombre de personnes est en outre concerné, l'autorité soumet le traitement à l'autorité de protection des données compétente en vue de sa prise de position (niveau 3, art. 20 P-LCPD).

13.7 Fichiers et obligation d'inscrire au registre

Le registre a donné lieu à des opinions très divergentes lors de la procédure de consultation. Certaines et certains (ACB, IG ländlicher Raum, Worb, Berne) ont accueilli favorablement le fait de limiter les inscriptions aux données personnelles sensibles, tandis que d'autres (JDB, Les VERT-E-S) ont souhaité que l'exploitation d'un profilage figure également au registre. Un cercle restreint de participantes et participants (AAB, Société Numérique, Thoune) souhaitait que le registre porte, comme maintenant, sur la totalité des traitements et un petit nombre d'avis (Langenthal, Groupe de l'Île) allait dans le sens d'une suppression totale de l'instrument. Différents cantons conservent un registre répertoriant l'ensemble des opérations (notamment Zurich et

Bâle-Ville), d'autres ont limité la portée de l'obligation aux autorités pénales (comme Bâle-Campagne ou Lucerne). La charge de travail et la difficulté de tenir un registre à jour ont notamment été critiquées. Le délégué à la protection des données peut toutefois sensibiliser les autorités et organiser simplement aussi bien la saisie que la mise à jour des informations. Dans un souci de réduction de la charge de travail, le contenu des registres est en outre limité aux données sensibles. Pour des questions de transparence, la règle doit être maintenue. En outre, l'exploitation de **profilages à risque élevé** par des autorités ou l'utilisation de **systèmes algorithmiques de prise de décision** (communément nommés «intelligence artificielle») présentant un risque élevé pour la personne concernée peuvent être particulièrement délicates. Par conséquent, ces traitements doivent également être rendus publics par les autorités.

13.8 Obligations d'annoncer en cas de violations de la sécurité des données

En droit européen, il existe à la fois des situations où la violation de la sécurité des données doit être annoncée en cas d'atteinte grave ou de risque élevé pour les personnes concernées seulement et des situations où un simple risque rend une annonce nécessaire. La loi fédérale, quant à elle, l'exige seulement si la violation entraîne un risque élevé pour la personne concernée. Il s'agit d'éviter l'annonce de violations insignifiantes. L'autorité doit évaluer dans tous les cas les conséquences de la violation pour la personne concernée. L'obligation d'annoncer est aussi réglée différemment selon les cantons: pour Zurich et Lucerne, par exemple, elle suppose un risque élevé ou important pour la personne concernée, tandis que le canton de Bâle-Campagne renonce à l'obligation seulement si la violation de la sécurité des données ne présente probablement pas de risque pour les droits fondamentaux de la personne concernée. Le projet soumis à la procédure de consultation exigeait une annonce même si la violation ne présentait aucun risque élevé pour la personne concernée car l'obligation ne devait pas être l'exception mais la règle. L'objectif était que l'autorité de protection des données puisse soutenir l'autorité dans les tâches garantissant la sécurité des données le plus tôt possible et de façon globale. Les destinataires de la procédure de consultation ont été plusieurs toutefois à demander que l'annonce ne soit obligatoire que si la violation est susceptible d'engendrer un risque **élevé** pour les droits fondamentaux de la personne concernée. Étant donné que la définition des cas soumis à l'obligation d'annoncer était manifestement trop peu restrictive, l'alinéa est adapté au droit fédéral.

13.9 Centralisation des autorités de protection des données

À l'occasion de la procédure de consultation, les avis divergeaient à propos de la centralisation partielle proposée. Elle a reçu un bon accueil dans neuf cas (PLR, association eGov, Thoune, Worb, ACB, Lyss, JDB, Les VERT-E-S, Berne) et trois prises de position adhéraient à une centralisation totale (Berthoud, Langenthal et Köniz, avec toutefois liberté de choix). Seules trois réponses se prononçaient en faveur du maintien de l'existence d'une autorité de protection des données propre à chaque commune et collectivité de droit communal (IG ländlicher Raum, UDC, commission de gestion de Muri).

Les cantons organisent le domaine de la surveillance de la protection des données de manière bien différente, mais ils ne sont qu'un tout petit nombre à prévoir une surveillance obligatoire au niveau communal. C'est le cas notamment du canton de Saint-Gall. La solution d'une décentralisation n'est pas maintenue, puisque seule une minorité s'est exprimée en sa faveur et qu'elle ne permet ni d'atteindre un haut niveau de protection ni d'utiliser les ressources avec efficience. L'option retenue dans le projet, c'est-à-dire celle d'une **centralisation partielle**, a l'avantage d'éviter que l'autorité cantonale de protection des données ne soit accaparée dans son travail par les plus grandes communes principalement. Il faut ajouter que ces dernières disposent déjà

de services de surveillance professionnels et bien établis, qui garantissent aujourd'hui déjà un niveau élevé de protection des données. Dans le canton de Zurich, la solution retenue est similaire dans la mesure où seules la ville éponyme et Winterthour ont leur propre autorité de surveillance. Le reste des communes, contrairement à ce que le projet législatif bernois prévoit, peuvent choisir si elles gèrent une autorité qui leur est propre. Cette possibilité a été écartée dès le début du processus législatif, car le canton aurait couru le risque de voir une mosaïque de circonstances locales et des différences qualitatives dans la pratique en matière de protection des données. La variante mise en consultation augmente le niveau de protection des données, **restant ainsi adéquate**.

13.10 Mesures administratives

13.10.1 Voie de droit

L'attribution au Tribunal administratif de la compétence en matière de recours a été contestée lors de la procédure de consultation. Étant donné que les autorités de protection des données pouvant rendre des décisions sont diverses (cantonale, de droit communal ou rattachées à une Église) une réglementation nuancée des instances est nécessaire.

Si une autorité de protection des données de droit communal rend une décision contre une commune ou une autre collectivité de droit communal, l'instance de recours pourrait aussi bien être la préfecture compétente que l'autorité cantonale de protection des données. L'autorité cantonale de protection des données exerce la haute surveillance (art. 43, al. 2 P-LCPD). Cependant, cette dernière ne confère justement pas la compétence d'agir en lieu et place des organes soumis à la haute surveillance, d'annuler ni de modifier des décisions (voir aussi l'art. 4 LGC). L'autorité cantonale de protection des données ne saurait donc se qualifier pour connaître des recours.

Selon le droit en vigueur, les décisions des communes ou d'autres collectivités de droit communal pourraient être attaquées devant la préfecture compétente (art. 26 LCPD et art. 63, al. 1, lit. *a* LPJA). Il appartient aux préfectures d'exercer la surveillance cantonale (art. 87 LCo). Il y a lieu de maintenir cette organisation juridictionnelle aussi pour les décisions des autorités de protection des données de droit communal. Deux communes et l'ACB se sont exprimées en faveur de cette solution, qui est mise en œuvre.

L'autorité cantonale de protection des données n'est subordonnée à aucune Direction. Elle est, à l'instar du Contrôle des finances, une unité administrative indépendante au sein de l'administration (voir le point 7.9.4). Par conséquent, le projet envoyé en consultation prévoyait que le Tribunal administratif soit l'instance de recours directe et ce, indépendamment de l'entité contre laquelle la décision est rendue (commune, autre collectivité de droit communal, y c. paroisses, ou autorité cantonale). Cette solution s'inscrit dans la droite ligne du guide de la CdC et correspond aux moyens de droit bernois. Les décisions du Contrôle des finances sont elles aussi attaquables devant le Tribunal administratif[142]. Dans la mesure où l'autorité cantonale de protection des données a compétence décisionnelle, le modèle ne sera pas modifié.

La question des recours contre les décisions des autorités de protection des données relevant d'une Église nationale doit aussi être réglée. Il ne s'agit pas là des paroisses en tant que collectivités de droit communal; dans ce cas, la surveillance est exercée par l'autorité cantonale de protection des données. Les décisions des autorités relevant d'une Église nationale rendues en vertu du droit temporel, qu'il soit seul applicable ou en complément au droit ecclésiastique, doivent être directement attaquées devant les instances prévues par la LPJA (art. 23 de la loi sur

[142] JAB 2023, p. 201. consid. 1.1

les Églises nationales bernoises [loi sur les Églises nationales][143]). Dès lors, la première instance de recours contre les décisions en matière de protection des données rendues par les Églises nationales est le Tribunal administratif (art. 74 LPJA).

13.11 Compétence décisionnelle à l'égard des tribunaux et du Ministère public

À plusieurs reprises, les parties prenantes à la procédure de consultation ont critiqué le fait que l'autorité cantonale de protection des données ne disposait pas d'une compétence décisionnelle à l'égard des tribunaux et du Ministère public (JDB, pvl, Les VERT-E-S, l'Union cantonale des arts et métiers «PME Bernoises», l'Union du commerce et de l'industrie).

Adapté sur la base de la procédure de consultation, le projet prévoit désormais que l'autorité cantonale de protection des données pourra également rendre des décisions contre les autorités judiciaires et le Ministère public (voir l'art. 47, al. 2 P-LCPD) dans le domaine d'application de la loi cantonale sur la protection des données (voir l'art. 3, al. 4 P-LCPD). Les décisions et les décisions sur recours de cette autorité peuvent être attaquées devant le Tribunal administratif dans les 30 jours. Ainsi, la compétence décisionnelle de l'autorité cantonale de protection des données est réglée de la même manière pour toutes les autorités.

À titre exceptionnel, une décision peut être portée devant la Cour suprême dans le cas où elle a été rendue par l'autorité cantonale de protection des données à l'encontre du Tribunal administratif.

Il est important de noter que la surveillance n'est exercée que là où la loi cantonale sur la protection des données s'applique (voir l'art. 3, al. 3 P-LCPD). L'existence de prescriptions procédurales est déterminante. Le traitement de données personnelles dans une procédure en cours devant les autorités judiciaires ou le Ministère public ne peut pas être surveillé par l'autorité de protection des données. Par contre, les autorités judiciaires et le Ministère public doivent soumettre au contrôle préalable de l'autorité de protection des données les traitements systématiques envisagés de données personnelles; à cette occasion, les questions d'ordre général sur le traitement sont abordées, comme la manière de gérer des données sur des personnes autres que celles visées.

Il convient encore de mentionner que l'autorité cantonale de protection des données n'a jusqu'à présent jamais donné lieu à une décision sur recours et, à l'avenir non plus, elle ne devrait pas rendre beaucoup de décisions. Son objectif est surtout de prodiguer des conseils.

14. Proposition

Le Conseil-exécutif propose au Grand Conseil d'adopter le projet de loi cantonale sur la protection des données (LCPD).

[143] RSB 410.11