Rapport

Date de la séance du CE : 21 juin 2023
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

Table des matières

1. Synthèse

Le droit à la protection des données est un droit fondamental. La loi cantonale sur la protection des données précise les garanties qu'apportent les Constitutions fédérale et cantonale à ce droit et donne corps à d'autres obligations internationales. Parmi ces garanties se trouve essentiellement 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.)[1] et que l'article 18 de la Constitution du canton de Berne du 6 juin 1993 (ConstC)[2] concrétise comme droit à la protection des données. L'ancrage constitutionnel révèle toute l'importance accordée à la protection des données; son origine repose sur la peur qu'inspire un contrôle des individus par l'État. Tel que prévu par les règles constitutionnelles, le respect du droit fondamental à la protection des données se traduit en particulier par un maniement adéquat et transparent des données personnelles, par la garantie qui doit être offerte aux personnes en matière de connaissance et d'influence ainsi que par la mise sur pied de contrôles appropriés.

Les autorités fédérales et les personnes privées sont soumises à la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[3]; s'agissant des autorités cantonales et communales, le

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

traitement de données personnelles est régi par leur propre législation sur la protection des données.

Le droit de la protection des données est mixte, 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 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 responsables 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 responsables 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 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

[4] RSB 152.04

[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)

(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 nº 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 nº 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 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 nº 108+. Elle entrera en vigueur en septembre 2023. À cette date, la loi sur la protection des données Schengen[11], qui garantissait l'acquis de Schengen, sera abrogée.

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 ordon-

[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 577
[8] FF 2020 5559
[9] RSB 152.043
[10] FF 2020 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)

nance 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 est introduit en tant que nouveau type de traitement des données.
- 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, notamment 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

Jusqu'ici, le droit prévoyait une exception de principe pour l'application de 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 responsables 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 dans le cadre d'une procédure concrète, indépendamment de tout traitement de données personnelles. 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. Néanmoins, elle n'a pas le pouvoir de décider de mesures administratives à l'encontre des tribunaux et du Ministère public, c'est-à-dire d'édicter une décision les concernant.

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 responsables 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 de données expose vraisemblablement les droits fondamentaux à un risque élevé (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 les droits fondamentaux de 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 responsable 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 le 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 responsable 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, 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 responsables 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	PC-révLCPD
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 sans référence aux personnes concernées
3 Fichiers	3 Obligations de l'autorité responsable 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 Autorités de protection des données de droit communal et des Églises nationales

			5.3 Tâches de l'autorité de protection des données
5	Procédure et protection juridique	6	Procédure et protection juridique
		7	Dispositions d'exécution
7	Dispositions finales	8	Dispositions transitoires et 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 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 PC-révLCPD). Dans le cadre de la révision, les lois indiquées ci-après sont modifiées.

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.

[12] Sur l'ensemble du sujet, voir les Directives sur la technique législative, module 3, chiffre 2.2.4.2
[13] RSB 109.1
[14] RSB 122.11
[15] RSB 122.20

3.8.4 Loi du 20 juin 1985 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 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 donnés 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 responsables 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 révLPD) et leur désignation

[16] RSB 152.01
[17] RSB 152.040.1

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 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 déroge pas, en fin de compte, dans son essence aux règles générales régissant la responsabilité de l'État[19]. Par conséquent, il n'y a pas lieu de la transposer dans le nouveau droit.

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 efficacité.

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 dans une ordonnance.

[18] RSB 551.1
[19] JAB 2008, p. 49, c. 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

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) avaient 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 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 les droits de 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 du traitement de données.

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 de données, 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 le mandat législatif.

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. L'évaluation prend la forme d'un rapport remis par les autorités de protection des données aux organes qui les élit (art. 48 PC-révLCPD).

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). La loi cantonale sur la protection des données précise les devoirs des autorités, c'est donc à elles que l'article premier, qui définit le but, s'adresse. Les autorités ne peuvent traiter des données personnelles qu'en adéquation avec la Constitution cantonale et la loi bernoise sur la protection de données.

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 physiques. 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 révLPD), 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)[20]. 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 bernoise sur la protection des données aux personnes physiques pour qu'en parallèle l'introduction de dispositions distinctes sur le traitement de données personnelles devienne nécessaire dans plusieurs lois spéciales. Selon l'article 5 Cst., le droit est la base de l'activité de l'État. La base légale exi-

[20] RS 172.010

gée 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. Il y a donc lieu de renoncer à une limitation du champ d'application. 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 champ d'application aux personnes physiques (le canton de Lucerne, p. ex.), ils ont introduit des dispositions particulières dans les lois spéciales.

Par rapport au droit actuel, l'article sur le but reste inchangé en français et connaît seulement des modifications d'ordre rédactionnel en allemand.

Article 2 – Définitions

La majeure partie des définitions coïncide avec celles de la législation en vigueur. Les ajouts et les divergences font l'objet des considérations qui suivent. Deux nouveaux termes sont introduits: le profilage et la violation de la sécurité des données. 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») 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 PC-révLCPD).

Lettre b

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 PC-révLCPD). 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.

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.

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[21]. 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 sur l'origine ethnique sont en revanche des données sensibles.

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[22].

Le Tribunal fédéral distingue, selon la théorie des trois sphères[23], 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])[24].

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, de la motricité, de la démarche ou encore de la voix. Ces données doivent impérativement résulter d'un traitement

[21] voir Rudin, Beat (2014). Praxiskommentar zum IDG des Kanton Basel-Stadt. Zurich, Bâle, Genève: Schulthess Médias Juridiques SA, note 37 ad § 3, note de bas de page 71
[22] 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, note 33 ad article 3
[23] ATF 97 II 100 s., c. 3 = JdT 1972 I 244; ATF 118 IV 45; ATF 119 II 222 ss., c. 2b
[24] RS 810.12

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[25].

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[26].

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[27]. 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 à leur encontre une mesure, 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, le séquestre d'animaux ou l'interdiction d'offrir des services selon la loi du 8 octobre 1999 sur les travailleurs détachés (LDét)[28].

Lettre c

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. 21 PC-révLCPD).

Lettre d

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. Comme le profilage est repris en tant que mode de traitement, le texte ne laisse aucun doute sur le fait qu'il ne s'agit pas d'un type de données personnelles. La notion est définie à la lettre *f*.

[25] FF 17.059, ch. 9.1.3.1, p. 6641
[26] voir Rudin, Beat (2015), in: Baeriswyl, Bruno/Pärli, Kurt (éd.), Datenschutzgesetz (DSG). Berne: éditions Stämpfli SA, note 27 ad article 3
[27] voir, pour le canton de Bâle-Ville au sujet de la notion de mesures d'aide sociale, Rudin, Beat (2014), *op. cit.*, note 38 ad § 3
[28] RS 823.20

Lettre e

Le terme de «communication» est repris sans changement et s'applique au fait de rendre des données personnelles accessibles. 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 f

Le profilage correspond à un mode spécial de traitement des données, 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 qu'il soit exploité par une autorité, un profilage à risque élevé ne dépend d'aucune exigence spéciale au sens de la loi fédérale révisée sur la protection des données. Pour le canton, la notion de profilage «simple» est seule déterminante, raison pour laquelle la définition introduite dans la loi cantonale sur la protection des données doit s'y rapporter. 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 simple. En ce sens, il s'agit d'un traitement automatisé de données personnelles servant à évaluer, à analyser ou à prédire certains aspects personnels relatifs à une personne physique.

Un profilage existe par exemple lorsque l'autorité établit un profil idéal de candidate ou de candidat pour un poste et qu'elle laisse le soin à l'ordinateur de juger la personne qui y correspond le mieux.

Selon le risque potentiel, le profilage doit satisfaire les mêmes exigences que celles imposées pour le traitement de données sensibles. Autrement dit, sans base inscrite dans la loi, il n'est pas possible (voir le commentaire de l'art. 4, al. 2 PC-révLCPD).

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

Lettre g

L'ordonnance portant introduction de la directive (UE) 2016/680 relative à la protection des données à caractère personnel a imposé l'obligation pour les autorités cantonales compétentes en matière de prévention, de poursuite pénale et d'exécution des peines de notifier les violations de la protection des données. Cette obligation doit être transposée dans la loi cantonale sur la protection des données (art. 25 à 27 PC-révLCPD). La notion de violation de la protection des données doit être définie en même temps que le reste de la terminologie. La teneur de la définition doit toutefois se rapprocher de la disposition fédérale (voir l'art. 5, lit. *h* révLPD). 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. Afin que la définition s'accorde avec la formulation retenue dans la loi sur la sécurité de l'information et la cybersécurité (LSIC)[29] qui doit être édictée au niveau cantonal, l'adjectif «illicite» de la définition fédérale est remplacé par «sans autorisation». Le terme se rapporte au fait qu'une sécurité adéquate des données doit être garantie lors de

[29] RSB [à déterminer]

leur traitement par des mesures techniques et organisationnelles appropriées (art. 10 PC-révLCPD).

Il y a violation de la sécurité des données lorsque les données personnelles traitées sont, de manière intentionnelle ou sans autorisation,

- perdues ou détruites (disponibilités des données personnelles),
- modifiées (atteinte à l'intégrité des données personnelles) ou
- divulguées ou rendues accessibles à des tiers non autorisés (confidentialité des données personnelles).

La disponibilité, l'intégrité ou la confidentialité des données sont affectées de manière imprévue, 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.

Lettre h

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 trop restrictive en partie et trop vaste. Le texte modifié explicite le fait que le terme d'autorités est entendu dans un sens très large 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 et que ces autorités jouissent d'une dérogation partielle en matière de surveillance (voir l'art. 3, al. 3 et l'art. 46, al. 4 PC-révLCPD).

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])[30].

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 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

[30] RSB 151.21

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])[31]. 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 en principe 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 publiques 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[32].

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)[33], comme c'est le cas aujourd'hui. Cette fois encore, le corps électoral est exclu du champ d'application.

Article 3 – Champ d'application

Alinéa 1

Comme jusqu'à présent, la loi cantonale sur la protection des données vaut pour chaque traitement de données personnelles, indépendamment des moyens ou des procédures utilisés. Cette disposition n'est pas modifiée.

Alinéa 2

Lettre a

À l'heure actuelle, les actes de l'autorité relevant de l'économie privée n'entrent pas non plus 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 toujours pas de raison pour que les règles de la loi cantonale sur la protection de données leur sont appliquées. Il y a donc lieu de reprendre telle quelle la teneur des dispositions du droit en vigueur (art. 4, al. 2, lit. *a* LCPD). Toutefois, les nouvelles prescriptions veulent que des règles relevant de la protection des données leur 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 données sont régis par

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

la loi fédérale sur la protection des données, ce qui n'a pas à être explicitement mentionné dans la loi cantonale. 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.

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 PC-révLCPD). La disposition concerne ainsi des autorités constituées en vertu du droit public (art. 2, al. 1, lit. *h*, ch. 1 et 3 PC-révLCPD).

Lettre b

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

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. La législation spéciale peut aussi limiter les principes de la protection des données, prévoir des exceptions ou préciser des règles ouvertes.

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 les procédures judiciaires, les procédures de justice administrative et les procédures réglées par des prescriptions procédurales particulières. Pour les procédures de justice administrative, c'est loi du 23 mai 1989 sur la procédure et la juridiction administratives (LPJA)[34] qui fait foi. Quant aux prescriptions procédurales particulières, il s'agit notamment de la loi du 1er février 2012 sur la protection de l'enfant et de l'adulte (LPEA)[35] 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 garantissent également la sauvegarde des droits fondamentaux de toutes les personnes impliquées, offrant ainsi une protection équivalente à celle de la législation

[34] RSB 155.21
[35] RSB 213.316

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 donc exclusivement régis par les prescriptions procédurales applicables lors de la procédure mentionnée, notamment par les dispositions du code de procédure civile du 19 décembre 2008 (CPC)[36], du code de procédure pénale suisse du 5 octobre 2007 (code de procédure pénale, CPP)[37] et de la loi sur la procédure et la juridiction administratives. Cela signifie que les droits de la personne concernée (4e titre PC-révLCPD) 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 parties à la procédure ou de celui effectué par les parties vis-à-vis d'autres parties. 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 parties. À titre d'exemple, les parties 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 parties. 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 des autres parties 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[38]. 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 qu'un vague soupçon. Cette dernière n'est pas régie par le code de procédure pénale[39]. 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'article 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][40]). 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

[36] RS 272
[37] RS 312.0
[38] voir FF 17.059, ch. 9.1.2, p. 6633
[39] Rapport du Conseil-exécutif concernant la loi sur la police (2017), commentaire de l'article 72, p. 40
[40] RSB 271.1

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 du 10 novembre 2004 réglant la communication des décisions pénales prises par les autorités cantonales[41]) soit dans un acte législatif spécial distinct.

Il découle de l'alinéa 3 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.

La prescription contenue à l'article 3, alinéa 3 PC-révLCPD ne vaut pas pour les procédures administratives (procédures préalables au prononcé d'une décision). C'est ce qu'indique la deuxième phrase de l'alinéa. Ce sont donc les dispositions de la loi cantonale sur la protection des données qui s'appliquent dans ces cas. La réglementation prévue par le droit actuel doit être conservée sans être modifiée.

Les tribunaux et le Ministère public ne sont pas soumis à la surveillance de l'autorité cantonale de protection des données dans la mesure où ils ne sont pas couverts par le champ d'application de la loi cantonale sur la protection des données. Dans les autres cas, s'ils sont donc tenus de respecter cette loi, l'autorité cantonale de protection des données n'a néanmoins pas le pouvoir de rendre des décisions à leur encontre (voir art. 46, al. 4 PC-révLCPD).

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 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, lit. *a* ConstC). Les communes peuvent aussi complètement déléguer cette compétence au parlement[42]. Il faut tenir compte du fait que le traitement de données sensibles et, parfois, la pratique du profilage exigent une base légale prévue dans une loi ou un règlement (voir les art. 2 et 3).

La base légale peut être directe ou indirecte. La base légale directe règle explicitement le traitement de données: elle oblige ou habilite l'autorité responsable à traiter certaines données personnelles[43]. L'article 39, alinéa 3 de la loi du 3 décembre 2020 sur les prestations particulières

[41] RS 312.3
[42] Wichtermann, Jürg (1999), in: Kommentar zum Gemeindegesetz des Kantons Bern. Berne: éditions Stämpfli, remarque sur la note 12 ad articles 50 à 60
[43] Rudin, Beat (2014), *op. cit.*, note 16 ad § 9

d'encouragement et de protection destinées aux enfants (LPEP)[44], 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 responsable une tâche qui peut être remplie seulement par le traitement de données personnelles[45]. 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 responsable. 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 et du profilage. 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 ou de procéder à un profilage que lorsqu'une base légale 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 aussi traiter des données personnelles ou entreprendre un profilage si l'accomplissement d'une tâche légale l'exige (base légale indirecte). Selon la législation en vigueur, il suffit que le traitement de données personnelles «serve» à accomplir une tâche légale. La teneur du texte suggère que le traitement de données personnelles doit seulement être utile à l'accomplissement d'une tâche, ce qui n'est pas juste. Conformément au principe de proportionnalité, le traitement de données doit être nécessaire pour que la tâche légale puisse être remplie, ce qui ressort désormais aussi du texte de la loi.

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 certains profilages. Étant donné qu'il existe aussi des profilages portant moins gravement atteinte aux droits fondamentaux des personnes concernées (voir le commentaire de l'art. 2, lit. *f* PC-révLCPD), les conditions supplémentaires au sens de l'alinéa 2 ne s'imposent que si la finalité du traitement implique des risques particuliers pour les droits fondamentaux de la personne concernée. Lorsqu'un profilage n'entraîne aucun risque particulier, une base légale directe ou indirecte au sens de l'alinéa 1 suffit. Si l'autorité responsable recourt au profilage et qu'il présente un risque particulier, il faut partir du principe qu'une atteinte grave est portée au droit fondamental à la protection des données et la situation doit être évaluée 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 dont la finalité implique des risques particuliers pour les droits fondamentaux des personnes concernées que s'il existe une base suffisamment précise dans la loi. La loi peut se limiter à régler les principes; il faut donc pouvoir en inférer de manière suffisamment

[44] RSB 213.319
[45] Rudin, Beat (2014), *op. cit.*, note 17 ad § 9

précise l'autorité responsable et la finalité du traitement ou du profilage, de même que les catégories particulières de données. Il n'est toutefois 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.

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 potentiellement un risque. L'accomplissement des tâches doit «impérativement» l'exiger. Les personnes concernées doivent être capables de déterminer les données sensibles traitées 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 suffisamment précise 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 des risques sont désormais aussi concernés.

Le fait qu'une base de rang inférieur (décret ou ordonnance) suffit lorsqu'une personne concernée consent au traitement des données (lit. *c*) doit également être repris. 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 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* révLPD). Cette exigence découle déjà des Constitutions fédérale et cantonale (art. 36, al. 1 Cst. et art. 28, al. 1 ConstC).

Alinéa 3

Le secret de fonction et 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 réservés. Il y a là une collision entre des normes juridiques: la loi cantonale sur la protection des données prévoit le traitement de données personnelles tandis que la loi spéciale prescrit le maintien du secret. Selon les règles de conflit générales qui s'appliquent dans ce cas, la loi sur la protection des données est une *lex generalis* sur laquelle prime la prescription en matière de secret en tant que *lex specialis*. La réserve de la loi cantonale sur la protection des données n'a par conséquent qu'un caractère déclaratoire. Elle figure toutefois déjà dans le droit en vigueur (art. 5, al. 5 LCPD) et est maintenue dans un souci de clarté.

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* révLPD). Le fait que le pouvoir exécutif puisse, s'il estime opportun, autoriser le traitement de données personnelles 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 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 PC-révLCPD). Il ressort des bases légales applicables à l'accomplissement des tâches. 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, tout comme l'archivage l'est dans la phase inactive (voir le commentaire de l'art. 16). 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 responsables et les personnes privées. Par conséquent, la communication de données personnelles par les autorités responsables 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 et puisse être exigé de la personne concernée. Il est donc indispensable que le but du traitement des données soit défini (art. 6 PC-révLCPD).

Article 8 – Exactitude

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 PC-révLCPD). 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 révLPD.

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[46].

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 droits fondamentaux des personnes concernées.

La norme matérialise l'approche fondée sur les risques. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, 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 élevées[47].

Alinéa 3

Cet alinéa introduit l'obligation de garantir, par des préréglages appropriés, que le traitement des données personnelles 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 de données 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 responsable prévoit plusieurs

[46] voir Rosenthal, David (2020). La nouvelle loi sur la protection des données, in: Jusletter du 16 novembre 2020, note 44
[47] FF 17.059, ch. 9.1.3.1, p. 6649

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 responsable peut donc décider qu'un traitement de données particulier ne peut être choisi que si d'autres traitements de données sont autorisés en même temps. Cette possibilité est au plus limitée par le principe de proportionnalité ou par la liberté de consentement[48].

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 révisée. 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 prévues, l'autorité responsable 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. Il appartient à l'autorité responsable 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

Le canton de Berne édicte 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)[49] 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 responsables prennent donc les mesures qui s'imposent selon le besoin de protection constaté pour garantir la confidentialité, la disponibilité, l'intégrité et la reconnaissabilité 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

[48] voir Rosenthal, David (2020), *op. cit.*, note 50
[49] RSB [à déterminer].

l'administration numérique, comportant une disposition à cet égard qui est en adéquation avec les prescriptions supérieures de 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 des données 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 loi 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 étant 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 responsable, 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 de données, 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 des données 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 garantit par ces moyens, de manière à ce 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 division des responsabilités.

À l'image du droit fédéral (art. 33 révLPD), 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. 44, al. 2, lit. *a* PC-révLCPD).

Article 12 – Traitement sur mandat

Les articles 22 et 23 de la directive européenne prescrivent de manière détaillées les conditions dans lesquelles le traitement par un tiers est licite. La directive impose notamment des exigences aux 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 révLPD. La loi fédérale propose désormais des règles pour la sous-traitance (art. 9, al. 3 révLPD). 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 responsable 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. Si des données sont transférées à cet effet à l'étranger, il faut en outre que les conditions prévues à l'article 15 PC-révLCPD soient remplies.

Alinéa 1

L'alinéa 1 institue un devoir de diligence à la charge de l'autorité responsable 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 responsable 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 l'externalisation des traitements de données personnelles repose

sur une loi ou un contrat n'est plus précisée. La délégation des traitements prévue par la loi débouche souvent sur la transmission de l'accomplissement même de la tâche, de sorte que la personne assumant finalement la tâche devient elle-même une autorité (au sens de la loi cantonale sur la protection des données).

Tant des dispositions légales que des obligations contractuelles peuvent s'opposer à un traitement de données confié à des tiers; d'où le fait, par exemple, que la conservation des données en Suisse soit explicitement prescrite. Les obligations de confidentialité sont prévues comme règle spéciale par l'alinéa 2.

Alinéa 2
Les obligations de garder le secret sont traitées spécifiquement. Le strict minimum dépend du service (s'il s'agit d'une simple solution de stockage, un accès n'est jamais nécessaire; s'il prend la forme d'un logiciel en tant que service [SaaS], les données ne doivent pas être protégées par un chiffrement durant le traitement). Les mesures techniques et organisationnelles doivent garantir le fait que l'accès soit tout le temps réduit au minimum. Ces mesures peuvent être cumulatives ou alternatives.

Alinéa 3

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 à ce que le traitement réponde aux exigences légales. Pour cette raison, les exigences en matière de sécurité des données sont mentionnées explicitement.

Alinéa 4

L'alinéa 4 prévoit que les tiers mandatés ne peuvent pas transmettre le mandat de traitement à d'autres tiers sans le consentement préalable de l'autorité responsable. 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 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 en principe pas recueillies auprès de personnes privées. L'expression «en principe» 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 responsable 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 responsables 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 7.5.3). 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 de données personnelles. 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 indirecte ou directe. 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 portant exécution d'un autre acte législatif. 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 PC-révLCPD).

Comme mentionné, l'autorité responsable ne peut pas traiter de données personnelles sans qu'une base juridique ne l'y autorise en vertu d'un consentement (voir le commentaire de l'art. 4 PC-révLCPD). Par contre, elle peut communiquer les données personnelles qu'elle a recueillies conformément au droit si la personne concernée a, en l'espèce, donné son consentement ou si elle a rendu ses données personnelles accessibles à tout le monde et ne s'est pas opposée expressément au traitement (lit. *c*). 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 PC-révLCPD prévoit une réserve à cet égard.

Par ailleurs, l'autorité responsable 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

Le nouveau droit continue de prévoir que l'autorité demandant les données personnelles est habilitée à les traiter dans la mesure où aucune obligation de garder le secret ne s'y oppose (lit. *b*). 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).

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 (variantes au choix)

Le Conseil-exécutif propose deux variantes en ce qui concerne la communication de données personnelles à l'étranger. En principe, les autorités responsables ont le droit de communiquer des données personnelles à l'étranger si un niveau adéquat de protection des données est assuré (al. 1 et 2); des conditions justifiant des exceptions sont prévues (al. 3). La différence entre les deux variantes repose sur ces conditions et découle de l'arrêt «Schrems II» du 16 juillet 2020, rendu par le Cour de justice de l'Union européenne (CJUE), selon lequel les États-Unis d'Amérique ne garantissent pas une protection des données équivalente à celle exigée par le droit européen. Cet arrêt a aussi des conséquences pour la Suisse: la possibilité d'utiliser des solutions en nuage proposées par des entreprises étasuniennes, comme Microsoft 365, devient incertaine.

La variante 1 correspond à l'article 15, alinéas 1 à 3, lettres *a* à *c*. Les conditions justifiant des exceptions sont très restrictives et le droit fondamental des personnes concernées à la protection de leurs données y a plus de poids que l'intérêt public que constitue l'utilisation de solutions en nuage étasuniennes par des autorités responsables.

La variante 2 prévoit une exception, à titre supplémentaire, avec la lettre *d* de l'alinéa 3. Cette exception vise à faciliter l'utilisation de solutions en nuage étasuniennes. Elle donne plus de poids à l'intérêt public que constitue l'utilisation de telles solutions par des autorités responsables qu'à l'atteinte aux droits fondamentaux des personnes concernées, jugée improbable dans cette variante.

Points concernant les deux variantes

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 révLPD, art. 17 STE n° 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 proportionnées 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.

Alinéa 2

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 révLPD.

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 révLPD, 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[50]. Cette disposition allège clairement la tâche des autorités responsables, 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.

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'a pas inclus les États-Unis d'Amérique dans sa liste positive (annexe 1 de l'ordonnance fédérale sur la protection des données, entrant en vigueur le 23 septembre 2023).

Ainsi, 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 responsables doivent 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

[50] FF 2017 6565, p. 6658

(comme le chiffrement des données personnelles, lit. *c*) ou pouvoir se fonder sur l'une des circonstances justifiant une exception visées à l'alinéa 3.

Selon les dispositions de la variante 1, 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.

Les exigences restrictives compliquent notablement l'utilisation de solutions en nuage étasuniennes pour les autorités responsables, raison pour laquelle le Conseil-exécutif soumet à la consultation une variante 2, qui prévoit une exception à cet égard (voir l'al. 3, lit. *d*).

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* révLPD), la loi cantonale sur la protection des données renonce à mentionner chacune des garanties. Elles comprennent notamment les clauses de contrat approuvées par le préposé fédéral à la protection des données et à la transparence (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 44, alinéa 2, lettre *a* PC-révLCPD, 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 responsable est possible, de sorte que le choix de ne pas reprendre la disposition sert à la mise en œuvre de la motion Vogt.

Alinéa 3

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 3 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 responsables.

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'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 responsable 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. Deux conditions doivent être réunies: la communication n'est admise que pour le cas d'espèce et le consentement doit être exprès. Le caractère explicite découle de l'article 17 STE nº 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* révLPD. 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* PC-révLCPD).

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 révision de 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.

Complément à propos de la variante 2

Lettre d

Toutes les autorités ou presque disposent d'un compte sur Twitter, YouTube ou Instagram et les logiciels comme Zoom ou Teams sont régulièrement utilisés dans le secteur de la formation depuis la pandémie de coronavirus. La jurisprudence européenne concernant le niveau de protection des données assuré par les États-Unis d'Amérique et l'appréciation qu'en a faite le Conseil fédéral rendent difficile l'utilisation de ces services, proposés par des entreprises étasuniennes, pour les autorités responsables. En effet, l'élément déterminant réside dans le lieu de traitement des données personnelles (Suisse, Union européenne ou États-Unis d'Amérique). Le Conseil-exécutif du canton de Berne soumet donc à la consultation une variante prévoyant des circonstances où une communication à l'étranger est possible sans qu'un niveau adéquat de protection des données ne soit exigé. L'idée avec cette variante est de refléter la réalité et de faciliter le recours à des solutions en nuage étasuniennes.

Une telle règle ne coïncide pas avec le droit fédéral, ni avec la législation des autres cantons autant qu'il soit possible d'en juger ; elle présente un avantage pour le canton de Berne, puisque l'utilisation des solutions en nuage étasuniennes est admise lorsque les conditions du traitement sur mandat sont réunies. Cela signifierait que les autorités responsables n'auraient que l'obligation de garantir la sécurité des données (art. 12, al. 3 PC-révLCPD). La sécurité se mesure au risque d'une atteinte des droits fondamentaux (art. 10, al. 1 PC-révLCPD). La variante 2 part du principe que les risques pour la protection des données que représenterait pour les personnes concernées l'utilisation de solutions en nuage venant des États-Unis d'Amérique sont de nature théorique et n'ont guère de signification en pratique. À ces risques s'opposent un grand intérêt public d'ordre pratique à l'utilisation des meilleures solutions en nuage du monde: elles permettent aux autorités d'atteindre leurs buts de transformation numérique plus rapidement qu'avec des logiciels conventionnels qui ne se trouvent pas dans le nuage, pour un bud-

get plus restreint également et de manière plus conviviale pour la clientèle. La pondération accordée aux accès aux données facilités, le cas échéant, pour les autorités de poursuite pénale étrangères et les services de renseignement d'autres pays, ainsi qu'aux possibilités restreintes de défense juridique en cas de violations de la protection des données dans un autre État, est de moindre importance.

L'utilisation de logiciels en nuage étasuniens est la norme, dans les foyers comme dans l'économie privée. Rares sont les personnes qui n'ont pas de compte Apple, Microsoft ou Google et les appareils qui s'y rapportent, et la plupart des entreprises ne pourraient plus fonctionner sans les logiciels en nuage étasuniens. Au vu des circonstances, la prise de risque relève de la société dans son ensemble selon la variante proposée ici par le législateur: si presque toutes les personnes, physiques ou morales, considèrent les risques en question proportionnés et supportables à titre privé, le canton a le pouvoir et la possibilité de le faire pour sa population. À la différence des privés, les autorités sont en effet liées par les principes fixés dans les textes constitutionnels, comme le principe de la légalité, de sorte que les situations ne sont comparables qu'avec beaucoup de circonspection. Cependant, le canton devrait aussi pouvoir prendre en considération l'appréciation des risques à titre privé et la présente variante est donc mise en consultation.

Article 16 – Destruction 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.

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 responsable 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)[51] et continuent d'être nécessaires à cette fin. L'accès aux données est autorisé uniquement aux fins prévues par la législation sur l'archivage.

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).

[51] RSB 108.1

Alinéa 2

Par l'alinéa 2, le législateur oblige les autorités responsables à déterminer au moyen d'un délai de conservation 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 responsable 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)[52]: 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 sécurité 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 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 responsable 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 sans référence aux personnes concernées

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 sans référence aux personnes concernées», est formulé de manière plus neutre.

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.

[52] RSB 811.01

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 responsable, 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.

Alinéa 2

L'autorité responsable peut communiquer, à certaines conditions, des données personnelles à des tiers qui désirent les traiter sans référence aux personnes concernées. Les exigences supplémentaires fixées à l'alinéa 2 doivent être garanties par contrat ou, lorsque cela s'avère judicieux, par décision[53].

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 responsable (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 PC-révLCPD (*Datensicherheit*).

7.3 Obligations de l'autorité responsable et des tiers mandatés

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

Alinéa 1

Le droit européen, plus précisément l'article 12 STE n° 108+ sur la modification de l'article 10, paragraphe 2 STE n° 108 et l'article 27 de la directive (UE) 2016/680, exige une analyse de l'impact du traitement de la part de l'autorité responsable et si des tiers sont mandatés. Il s'agit essentiellement d'une auto-évaluation de l'autorité responsable, qui consiste en un examen, sous l'angle du droit de la protection des données, des traitements de données personnelles répétés qui sont envisagés et qui semblent quelque peu délicats. 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.

[53] Voir l'article 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)

Une disposition comparable existe au niveau fédéral: l'article 22 révLPD. Selon cet article, chaque traitement fait l'objet d'une analyse d'impact déterminant s'il est susceptible d'entraîner un risque élevé pour les droits fondamentaux de la personne concernée, ce qui implique une certaine charge de travail. Toutefois l'analyse des risques ne connaît pas d'exigences élevées. Il suffit d'une note dans le dossier du projet lorsque les traitements de données personnelles qui s'y inscrivent ne présentent pas de risques particuliers et qu'aucune mesure spécifique n'a donc besoin d'être prise. Le droit qui prévalait jusqu'à présent ne prévoyait pas explicitement une telle analyse, mais elle devait déjà avoir lieu dans le cadre du contrôle préalable.

Dans le cadre de l'utilisation des TIC par l'administration cantonale, il fallait évaluer, durant la phase d'«analyse préliminaire», si le projet présentait 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 de l'ordonnance de Direction du 3 janvier 2011 concernant la sûreté de l'information et la protection des données, OD SIPD)[54]. Selon les termes de cette ordonnance, si l'analyse met en lumière des exigences SIPD poussées, un concept SIPD qui définit les mesures organisationnelles et techniques supplémentaires nécessaires est à élaborer durant la phase de «conception» (art. 5, al. 5 OD SIPD). Sur ce point, une base est désormais inscrite dans la loi pour définir ce que l'on entend sans équivoque par 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. Contrairement au texte de loi fédéral, la liste est exhaustive.

D'après le droit européen, repris à l'article 22, alinéa 2 révLPD, 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.

La loi fédérale sur la protection des données précise par ailleurs qu'un tel risque existe notamment dans le cas d'un traitement de données sensibles à grande échelle et d'une surveillance systématique de grandes parties du domaine public (art. 22, al. 2, lit. *a* et *b* révLPD). Ces éléments doivent être repris dans le droit cantonal (lit. *a* et *b*).

Il existe également un risque élevé en présence d'obligations légales particulières de garder le secret (lit. *c*). Cette condition doit être reprise des prescriptions actuelles du droit concernant le contrôle préalable et complétée par rapport à la législation fédérale. Comme aujourd'hui, les obligations de ce genre sont notamment celles prévues en matière d'assurances sociales. N'en font pas partie les obligations contractuelles librement consenties, ce que l'ajout de «légales» traduit clairement.

Les moyens techniques mentionnés à la lettre *d* doivent être définis dans le détail par voie d'ordonnance. Il s'agit par exemple de données personnelles enregistrées sur des supports de données que la personne concernée porte sur elle.

Par rapport à la législation actuelle (à propos du contrôle préalable), le cas prévu pour les bases juridiques pour lesquelles il existe une incertitude est absent (art. 17a, al. 1, lit. *a* LCPD). Étant donné que l'autorité responsable ne peut traiter que des données personnelles pour lesquelles il existe une base juridique suffisante, le but et le sens de la disposition ne sont pas clairs. Le rapport sur l'introduction de la disposition n'entre pas non plus dans le détail. Au vu du manque de cas d'application, la disposition n'est pas reprise dans le nouveau droit, ce qui permet de mettre en œuvre la motion Vogt.

[54] RSB 152.040.2

Alinéa 3

Si l'autorité responsable constate lors de l'auto-évaluation que le projet présente un risque élevé, elle entreprend une analyse d'impact formelle. La législation cantonale connaissait déjà une analyse du genre avec le concept SIPD.

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 les droits fondamentaux à la protection des données de la personne concernée (lit. *b*) ainsi que les mesures prévues pour les protéger (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 de données personnelles ou au moins de les restreindre. La limitation de l'accès aux données ou la garantie de la sécurité des données en sont des exemples.

Article 20 – Contrôle préalable

Alinéa 1

Si l'analyse de risques montre que le traitement des données envisagé présente un risque élevé pour les droits fondamentaux de la personne concernée, l'autorité responsable le soumet avant son début à l'autorité de surveillance en vue de sa prise de position. La disposition s'appuie sur celle que le projet de la révision de la 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 présente un risque élevé pour les droits fondamentaux de la personne, et pas seulement lorsqu'il existe un tel risque malgré les mesures prises par l'autorité responsable. Sur ce point, la loi cantonale sur la protection des données s'écarte de la teneur de l'article 23 révLPD.

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 révLPD). 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 responsable est ainsi plus efficace, puisque les possibles champs problématiques d'un point de vue de la législation sur la protection des données sont ainsi détectés à un stade précoce du traitement des données 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 sont définis par voie d'ordonnance.

Alinéa 3

L'article 23, alinéa 2 révLPD 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 de Berne, 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 – Registre des fichiers

L'article 24 de la directive (UE) 2016/680 oblige l'autorité responsable et les tiers qu'elle a mandatés à tenir un registre de toutes les activités des traitements. Le champ d'application de la directive se limite toutefois à la prévention et 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 responsables 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 révLPD).

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 seules les données sensibles seront répertoriées. Cela 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 PC-révLCPD). À cela s'ajoute le fait que l'obligation d'informer au sens de l'article 23 PC-révLCPD peut être remplie par la mention de la publication des fichiers.

Alinéa 1

L'autorité cantonale de protection des données tient et met à jour un registre des fichiers cantonaux (art. 42, al. 2 PC-révLCPD) qui contiennent des données sensibles. Pour tenir ce registre, elle 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. À l'avenir, seuls les fichiers contenant des données sensibles seront consignés dans le registre. En général, ce sont ces fichiers qui revêtent un intérêt particulier pour les personnes concernées.

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, qui feront l'objet d'une publication après un contrôle de l'autorité cantonale de protection des données. Le registre aide la personne concernée à savoir où sont éventuellement traitées des données sensibles 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.

Alinéa 2

Les autorités de droit communal et celles des Églises nationales doivent tenir elles-mêmes leurs registres. Des standards définissant la manière dont il faut remplir cette obligation sont toutefois fixés par l'autorité cantonale de protection des données.

Alinéa 3

Le Conseil-exécutif fixe par voie d'ordonnance le contenu du registre, de même que les exceptions à l'obligation d'annoncer et à celle de consigner les données. S'agissant du contenu, il convient de garder les mêmes exigences qu'aujourd'hui. Les éléments suivants sont à mentionner en particulier: la base légale, l'autorité responsable, le but du traitement ainsi que la nature et l'étendue des données personnelles traitées, les catégories de destinataires et le délai de

conservation. Par exemple, le but indiqué peut être: «Examen du droit à la réduction des primes» ou «Profilage». Les catégories des données personnelles traitées désignent la nature des données (données sensibles, p. ex.). Le registre doit également indiquer les catégories des destinataires auxquels les données sont susceptibles d'être communiquées. On entend par là des groupes partageant les mêmes caractéristiques («autorités de surveillance», p. ex.).

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.

Article 22 – Obligation des autorités pénales 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, ainsi que les tiers qu'elles ont mandatés, 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. Les contenus du registre et les exceptions à l'obligation d'y inscrire les fichiers sont réglés dans une ordonnance du Conseil-exécutif. 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 responsables 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 responsable 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 cas exceptionnels pour lesquels 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,
- la manière de remplir l'obligation d'informer 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». Des informations additionnelles sont aussi nécessaires dans des cas exceptionnels, par exemple lorsqu'il existe un risque élevé d'abus dans le traitement de données.

L'obligation d'informer s'applique seulement dans la mesure où l'autorité responsable «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 de données.

Alinéa 3

Les modalités d'accomplissement du devoir d'informer sont réglées à l'alinéa 3. L'information peut être diffusée par trois canaux:

- le registre des fichiers,
- le site Internet de l'autorité responsable ou
- une communication directement adressée à la personne concernée.

Le canal à privilégier dépend du type de collecte des données. Si les données proviennent directement de la personne concernée, la publication dans le registre des fichiers ou sur un site Internet suffit. Dans tous les cas, l'autorité responsable doit veiller à ce que la personne concernée puisse effectivement prendre connaissance de l'information par un moyen facilement accessible, 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

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

- lorsque la personne concernée dispose déjà des informations (lit. *a*) ou
- lorsque l'acquisition de données personnelles est prévue par la loi (lit. *b*).

La collecte de données personnelles est prévue par la loi lorsque la personne concernée peut déduire à un degré suffisant de précision des bases légales quelles données sont traitées et dans quel but. L'obligation d'informer tombe alors dans la plupart des cas. 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).

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.

Alinéa 2

Il est également possible de limiter l'obligation d'informer aux mêmes conditions que celles qui s'appliquent 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 révLPD 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).

Article 25 – Annonce des violations de la sécurité des données à l'autorité de protection des données

Alinéa 1

Selon le droit européen, l'autorité responsable 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 expliqué dans le commentaire de l'article 2, lettre *h* PC-révLCPD. L'annonce doit avoir lieu au plus vite, mais dans un délai maximal 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 responsable 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 responsable.

La teneur de la loi fédérale sur la protection des données récemment adoptée prévoit que l'annonce est obligatoire dans les seuls cas où la violation entraîne vraisemblablement un risque élevé pour les droits fondamentaux des personnes concernées. Selon le droit cantonal, un risque vraisemblable suffit puisque l'obligation d'annoncer doit être la règle et non l'exception. L'objectif est que l'autorité de protection des données puisse soutenir l'autorité responsable dans les tâches garantissant la sécurité des données le plus tôt possible et de façon globale. Par ailleurs, l'article 30, paragraphe 1 de la directive (UE) 2016/680 ne prévoit qu'une exception: lorsqu'il est peu probable que la violation engendre un risque.

Alinéa 2

L'obligation d'annoncer correspond dans sa teneur à l'article 24, alinéa 2 révLPD. L'annonce doit décrire la violation et ses conséquences tout en indiquant les mesures prises ou envisagées. L'autorité veille à modifier son annonce dès que l'état de ses connaissances évolue.

Alinéa 3

En cas de sous-traitance, l'autorité responsable doit être informée de la violation par les tiers mandatés.

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 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 pour les droits fondamentaux des personnes concernées 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.

Une exception est aussi admise s'il est impossible de respecter l'obligation d'informer ou que l'information nécessiterait des efforts disproportionnés (lit. *c*). L'obligation d'informer est réputée impossible à respecter lorsque l'autorité responsable n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données, par exemple parce que les fichiers journaux qui permettraient une identification ne sont plus disponibles. De même, on estime que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées. C'est notamment dans ces cas de figure 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 responsable.

Alinéa 2

Il convient de renoncer à toute information 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* révLPD). 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.

7.4 Droits de la personne concernée

Article 28 – Droit d'accès

Alinéa 1

Le droit d'accès, c'est à dire de savoir si des données à son sujet sont traitées par une autorité responsable ou si cette dernière a mandaté un tiers pour le faire, et le cas échéant de connaître les données concernées 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 à 24 PC-révLCPD. La personne concernée peut en apprendre plus que ce que l'autorité responsable est tenue de lui communiquer si elle en fait la demande.

Alinéa 2

Le droit d'accès est un droit subjectif inhérent à la personne, que même une personne qui n'a pas l'exercice des droits civils mais qui est capable de discernement peut faire valoir seule, sans avoir à requérir le consentement de sa représentante légale ou de son représentant légal.

Le fait que ce droit est inhérent à la personne a pour conséquence que nul ne peut y renoncer par avance.

Alinéa 3

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

Article 29 – Contenu et modalité 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 sont les mêmes que celles devant être transmises par l'autorité responsable en cas de collecte de données (lit. *a*), auxquelles s'ajoutent la mention du délai de conservation (lit. *b*) et l'origine des données personnelles (lit. *c*). 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 responsable 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. 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 par conséquent 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.

Article 30 – Restrictions au droit d'accès

Lettres a et b

L'article règle les restrictions au droit d'accès. Sous le régime du droit en vigueur, un renseignement peut être refusé, limité ou différé 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 révLPD, l'autorité responsable 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 sûreté 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* révLPD).

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. Il faut alors procéder à une pesée des intérêts en présence.

Lettre c

La lettre *c* est nouvelle. Un refus, une restriction ou un report est possible si la demande d'accès est manifestement infondée ou procédurière. L'exception doit être interprétée de manière restrictive à deux égards: d'un côté, l'autorité responsable ne doit pas conclure à la légère au caractère manifestement infondé, voire procédurier, de la demande; de l'autre, c'est à elle qu'il revient de choisir l'option la plus favorable pour la personne concernée dans le cas où la requête serait manifestement infondée ou procédurière. Dans la mesure du possible, elle doit se contenter de restreindre la communication des renseignements, mais peut aussi, au besoin, la différer.

Il n'est pas nécessaire de justifier d'un intérêt particulier pour invoquer le droit d'accès. L'autorité responsable 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[55]. Le droit d'accès ne peut être limité que dans la mesure où il est constaté, sans examen approfondi, que la demande est manifestement infondée.

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 responsable dont elle sait pertinemment qu'elle ne traite pas de données la concernant. Dans ce cas non plus, l'autorité responsable 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 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. 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 PC-révLCPD). De plus, il y a traitement illicite lorsque, par exemple, il ne repose sur aucune base légale, il est disproportionné ou sa finalité ne correspond par au but originel du traitement. 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. 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 PC-révLCPD).

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 révLPD. 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.

[55] ATF 138 III 425, c. 5.4 s.

Alinéa 2

L'autorité responsable 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 PC-révLCPD).

Alinéa 3

L'alinéa a fait l'objet d'une adaptation terminologique pour mieux correspondre à la teneur de l'article 41, alinéa 4 révLPD: «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. Le traitement est par conséquent limité puisque les données ne peuvent 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 d'opposition à la communication à des personnes privées

La personne concernée qui prouve un intérêt légitime peut s'opposer à ce que l'autorité responsable communique les données personnelles qu'elle traite. 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 responsable est tenue, par des règles de la législation spéciale, de communiquer les données ou lorsque le blocage est abusif (p. ex. comme moyen d'éviter une poursuite).

7.5 Autorités de protection des données

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»[56]. 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 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).

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

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)[57]. 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 lui soumettre un rapport une fois l'an (art. 48 PC-révLCPD). 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.

Article 35 – Direction de l'autorité cantonale de protection des données

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

[57] RSB 622.1

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 PC-révLCPD). 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 plus dans la situation où le choix revient à l'entité contrôlée. La participation du pouvoir exécutif permet toutefois d'accorder une importance de premier plan aux compétences professionnelles des candidates et candidats plutôt qu'à leur appartenance politique. L'implication conjuguée des deux organes garantit une représentation équilibrée des différents intérêts. Il convient donc de laisser le système bernois tel qu'il est aujourd'hui, c'est-à-dire de concevoir l'élection comme étant de la responsabilité du Grand Conseil, qui se prononce sur la base des candidatures proposées par le Conseil-exécutif.

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. 58 PC-révLCPD).

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 – Préparation de l'élection ou de la réélection de la déléguée ou du délégué à la protection des données

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* du règlement du Grand Conseil du 4 juin 2013 [RGC[58]]). À présent, l'organe législatif ne participe pas à la préparation de l'élection. Or un processus sans heurts dépend de l'implica-

[58] RSB 151.211

tion des parlementaires dans la sélection des candidates et des candidats, ainsi que de la possibilité de s'exprimer sur leurs qualifications. À l'occasion de l'élection du délégué en fonction depuis mars 2019, une commission ad hoc a été mise sur pied. Cet organe comptait en son sein

- le président de la Commission de gestion,
- le chancelier et
- une représentation de la Direction de l'intérieur et de la justice composée d'un membre du Secrétariat général et du responsable du personnel.

Les expériences faites avec la commission électorale instituée étaient positives. L'implication des milieux politiques et administratifs a permis de tenir compte des différentes compétences de manière appropriée. La composition envisagée de la commission se fonde donc sur la structure qu'a connue celle instituée pour l'occasion en 2018. Elle comprend au moins les représentantes et les représentants mentionnés. La Direction de l'intérieur et de la justice peut inclure d'autres personnes au besoin.

Pour le moment, la proposition du Conseil-exécutif est soumise à la Commission de justice, qui la préavise à l'intention du Grand Conseil. Une telle préparation 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 (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 autre projet législatif.

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

Une voix prépondérante n'a pas besoin d'être prévue dans la législation. Il est tout à fait possible que la commission électorale propose plusieurs noms. L'organe électoral est le Grand Conseil. La décision lui revient donc.

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)[59]. 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. De plus, 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.

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 PC-révLCPD). 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 léga-

[59] RSB 153.01

lité, 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 manquement grave ou répété 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'a 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, 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)[60].

Article 41 – Organisation et statut

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 (al. 3). Seules les communes et autres collectivités de droit communal comptant plus de 25 000 habitantes et habitants 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. La nouvelle répartition des tâches est financée par l'intermédiaire de la compensation des charges (voir le commentaire de l'art. 57 PC-révLCPD).

[60] RSB 620.03

Article 42 – Tâches

Alinéa 1

Cet article résume en une liste condensée toutes les tâches des autorités de protection des données. Il vaut également dans le cas des communes et des autres collectivités de droit communal pour autant qu'elles soient tenues de désigner leur propre autorité.

Les autorités de protection des données soutiennent les autorités responsables 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, sécurité des données incluse. Les conseils visent à faire en sorte que les autorités responsables 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. 44 PC-révLCPD). L'objectif de la surveillance est de déceler les potentielles irrégularités et d'indiquer là 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 droits fondamentaux 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 PC-révLCPD). 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 de droit 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. 44, al. 4 PC-révLCPD).

Lettre d

Le rôle de l'autorité de protection des données est surtout de dispenser des conseils. Elle conseille les autorités responsables 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 ces deux entités, 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 PC-révLCPD). 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 autres mesures des communes et d'autres collectivités de droit communal qui n'ont pas d'autorités de protection des données propres (voir l'art. 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. 47 PC-révLCPD).

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. 48 PC-révLCPD).

Alinéa 2

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

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 des autres 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'Office des affaires communales et de l'organisation du territoire, 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 – Secret de fonction dans l'accomplissement des tâches

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 44 – Contrôle du respect des dispositions en matière de protection et de sécurité 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, sécurité des données incluse (art. 44 PC-révLCPD; actuellement: méthode de travail et procédure), recommandations (art. 45 PC-révLCPD) et mesures administratives (art. 46 PC-révLCPD).

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 et de la sécurité des données. Cet examen a lieu dans le cadre du contrôle préalable au sens de l'article 20 PC-révLCPD. 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.

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 PC-révLCPD) et la procédure de mise en œuvre de la sûreté 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 (voir l'art. 10 PC-révLCPD).

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 responsable 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 45 – 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. 46 PC-révLCPD). Il doit toutefois rester possible pour elle de faire part de ses recommandations à l'autorité responsable.

Du fait de l'obligation de motiver, l'autorité responsable 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. Le pouvoir décisionnel de l'autorité est caduc.

Article 46 – 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 responsables ont la possibilité de le faire en attaquant directement leurs actions. Elles peuvent utiliser les voies de droit normales à cet effet. La déléguée ou le délégué à la 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

L'autorité de protection des données n'est subordonnée à aucune Direction. L'article 34, alinéa 3 prévoit simplement un rattachement administratif à la Direction de l'intérieur et de la justice. Par conséquent, le moyen de droit doit être adressé directement au Tribunal administratif. Ce moyen de droit correspond à la proposition faite dans le guide pratique CdC.

Alinéa 3

Conformément à l'article 80, alinéa 1 LPJA, le Tribunal administratif ne dispose pas d'un plein pouvoir de cognition, c'est-à-dire qu'il ne peut examiner que les recours pour constatation inexacte ou incomplète des faits ou pour d'autres violations du droit, y compris celles qui sont commises dans l'exercice du pouvoir d'appréciation. L'inopportunité échappe à l'examen juridique du Tribunal administratif sauf dans des cas que la loi prévoit (art. 80, al. 1, lit. *c*, ch. 3 LPJA). Comme le Tribunal administratif est la seule instance prévue, il doit au moins disposer d'un plein pouvoir de cognition, raison pour laquelle l'alinéa 3 inscrit les griefs pour inopportunité dans la loi.

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.

Alinéa 4

La surveillance n'est effective que là où la loi cantonale sur la protection des données s'applique (voir l'art. 3, al. 3 PC-révLCPD). L'autorité de protection des données ne peut surveiller le traitement de données personnelles dans le cadre d'une procédure pendante devant les autorités judiciaires ou le Ministère public. Par contre, ils doivent soumettre les traitements de données systématiques envisagés au contrôle préalable de l'autorité de protection des données; à cette occasion, les questions générales de protection des données sont abordées, comme celle portant sur la manière de gérer les données qui concernent d'autres personnes que celle qui est visée. L'autorité de protection des données ne doit toutefois pas avoir la possibilité de prendre des décisions contraignantes à leur encontre, raison pour laquelle elle n'a pas le pouvoir d'ordonner des mesures administratives. L'accent est mis sur les activités de conseil.

Article 47 – 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. 51 PC-révLCPD). 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.

Alinéa 2

Comme jusqu'à présent, il est possible pour des autorités 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.

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.

Alinéa 4

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.

Article 48 – Rapport et information du public

Cet article porte sur le rapport annuel qui doit être soumis à l'organe électoral 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 s'adresse à l'organe électoral. Toutefois, l'autorité cantonale de protection des données le publie aujourd'hui déjà sur Internet. 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* PC-révLCPD) et de la législation sur l'information, de sorte qu'il n'est pas nécessaire de prévoir une règle explicite à cet égard.

S'il en va de l'intérêt général, 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 PC-révLCPD 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 49 – Dispositions applicables

Le principe inscrit à l'article 49 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, le Tribunal administratif est compétent (voir l'art. 46, al. 2 PC-révLCPD).

Article 50 – 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 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 responsable. 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.

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. Les principales procédures concernées sont celles qui découlent des articles 28 ss PC-révLCPD, 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 51 – 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 PC-révLCPD) 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.

Article 52 – 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 53 – 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. Toutefois, une exception est possible lorsque les requêtes présentent un caractère excessif ou procédurier.

Selon la teneur actuel de l'ordonnance du 22 février 1995 fixant les émoluments de l'administration cantonale (ordonnance sur les émoluments; OEmo)[61], un émolument est déjà exigé de la personne requérante qui était à l'origine d'un traitement de données illicite (art. 33, al. 2 OEmo) en cas de demande de rectification ou d'autres prétentions relatives à la protection des données. Cette exception doit à présent être inscrite dans la loi et, en même temps, étendue aux demandes de renseignement dans le but de prévenir les requêtes d'accès abusives. L'alinéa 2 offre par conséquent la possibilité au Conseil-exécutif de prévoir des exceptions à la gratuité. Ainsi, il est tenu compte du fait que certaines demandes de renseignement occasionnent un volume de travail considérable au responsable du traitement.

7.7 Dispositions d'exécution

Article 54 – Dispositions d'exécution

Cette disposition confère au Conseil-exécutif le pouvoir d'édicter les dispositions d'exécution nécessaires. De plus, elle souligne qu'il peut déléguer aux Directions des compétences de nature plutôt technique et opérationnelle ou relevant principalement des responsabilités des différentes autorités compétentes.

7.8 Dispositions transitoires et dispositions finales

7.8.1 Dispositions transitoires

Article 55 – Traitements en cours

La disposition transitoire concerne les traitements de données qui ont débuté sous l'ancien droit et qui perdurent après l'entrée en vigueur du nouveau droit. 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

[61] RSB 154.21

- Article 19: Analyse d'impact relative à la protection des données personnelles
- Article 20: Contrôle préalable

Ces articles portent sur les obligations des autorités responsables lors de la phase précédant le traitement. Elles n'ont pas à assumer ces obligations rétroactivement.

Article 56 – 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 de première instance, 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 57 – 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[62]: 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, de 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

[62] 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])

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 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.

Article 58 – La déléguée ou le 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).

7.9 Modifications d'autres actes législatifs

7.9.1 Loi du 19 février 1986 sur la protection des données (LCPD)[63]

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)[64]

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. 47 PC-révLCPD). 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,

[63] RSB 152.04
[64] RSB 109.1

les dispositions qui se trouvent dans la loi valent pour l'ensemble des traitements de données personnelles.

7.9.3 Modification indirecte de la loi du 12 septembre 1985 sur l'établissement et le séjour des Suissesses et des Suisses (LES)[65] 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)[66]

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 PC-révLCPD 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 PC-révLCPD, 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)[67]

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

[65] RSB 122.11
[66] RSB 122.20
[67] RSB 152.01

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 a entré raisonnablement 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)[68]

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)[69] et de la loi cantonal du 10 juin 2020 sur les jeux d'argent (LCJar)[70]

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[71]. 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)[72]. 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[73] et 111, alinéa 2 LPASoc[74] (voir l'art. 2, al. 1, ch. 6 PC-révLCPD).

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:

[68] RSB 555.1
[69] RSB 860.2
[70] RSB 935.52
[71] voir Rudin, Beat (2014), *op. cit.*, note 38 ad § 3
[72] RSB 860.1
[73] RSB 935.52
[74] RSB 860.2

- Article 29 de la loi du 2 novembre 1993 sur l'information et l'aide aux médias (LIAM)[75]
- Article 14 et article 20 de la loi du 31 mars 2009 sur l'archivage (LArch)[76]
- 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)[77]
- Article 12a de la loi du 16 septembre 2004 sur le personnel (LPers)[78]
- Article 35 de la loi du 18 mai 2014 sur les caisses de pension cantonales (LCPC)[79]
- Article 23 de la loi du 23 mai 1989 sur la procédure et la juridiction administratives (LPJA)[80]
- Article 55 de la loi du 1er février 2012 sur la protection de l'enfant et de l'adulte (LPEA)[81]
- 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)[82]
- Article 130 de la loi du 13 juin 2013 sur les soins hospitaliers (LSH)[83]
- Article 57g et article 80g de la loi du 11 juin 2001 sur l'aide sociale (LASoc)[84]
- 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)[85]

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 les programmes d'action sociale et de la loi cantonale sur les jeux d'argent.

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 n° 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.

[75] RSB 107.1
[76] RSB 108.1
[77] RSB 152.05
[78] RSB 153.01
[79] RSB 153.41
[80] RSB 155.21
[81] RSB 213.316
[82] RSB 271.1
[83] RSB 812.11
[84] RSB 860.1
[85] RSB 861.1

Les charges supplémentaires du canton sont toutefois remboursées par la compensation des charges (voir le commentaire de l'art. 57 PC-révLCPD). 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. 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.

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. 57 PC-révLCPD).

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 leur mandataire. 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

14. Proposition

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