Kommission für Staatspolitik und Aussenbeziehungen
Commission des institutions politiques et des relations extérieures
05.11.2024

Loi sur la sécurité de l'information et la cybersécurité

Informations complémentaires pour la 1re lecture

Sommaire

1. Objet

La Commission des institutions politiques et des relations extérieures (CIRE) a procédé en octobre 2024 à un examen préalable de la loi sur la sécurité de l'information et la cybersécurité en vue de la première lecture lors de la session d'hiver 2024. Elle a ensuite demandé à la Direction des finances de répondre à des questions supplémentaires, dans une volonté de mettre les réponses à la disposition du Grand Conseil pour la première lecture.

En vertu de l'article 16 du règlement de la Commission, la CIRE a publié le présent document par décision du 11 novembre 2024.

2. Questions de la CIRE du 25 octobre 2024 et réponses de la Direction des finances

2.1 Avancement des travaux dans les cantons

Question : mise à jour des informations (cf. chap. 6.2 du rapport) sur la base de l'enquête réalisée sur mandat de la CIRE et des nouvelles données reçues entretemps qui peuvent être publiées.

Après avoir examiné la LSIC pour la première fois le 16 octobre 2023, la CIRE a chargé la Direction des finances d'évaluer la situation et de clarifier les intentions des autres cantons. L'Office d'informatique et d'organisation (OIO) a alors réalisé à très courte échéance une enquête auprès des autres cantons, plus précisément de leurs services chargés de la sécurité. La Direction des finances a présenté les résultats de l'enquête à la CIRE lors de la séance du 22 octobre 2023, sur la base des réponses reçues à cette date de la part de onze cantons.

Davantage de réponses ont été transmises après cette séance, de sorte que les avis des cantons, sur la base des réponses données par 17 cantons, peuvent être résumés ainsi :

a) Huit cantons prévoyaient d'édicter leur propre loi sur la sécurité de l'information (AG, BE, FR) ou un autre acte législatif cantonal (AI, BL, NW, ZG, ZH).
b) Deux cantons n'avaient pas encore déterminé la procédure législative (GE, SG).
c) Huit cantons n'avaient prévu aucune adaptation législative (NE, GR, JU, LU, SH, SO, UR, VS).
d) Quatre cantons souhaitaient appliquer directement la LSI pour ce qui concerne les dispositions applicables aux cantons (NE, SH, UR, VS).

Conformément à ce qui avait été envisagé lors de la séance de la commission du 22 octobre 2023, l'OIO a organisé à l'automne 2024 des entretiens avec chacun des services spécialisés des cantons qui avaient identifié un besoin de légiférer. Voici en résumé ce qui a été discuté lors de ces échanges :

a) **Argovie :** le projet de loi argovien (« InfoSIG ») a été mis en consultation de mai à mi-août 2024. Il est prévu entre autres de le rendre applicable aussi aux communes et aux autres organisations chargées de tâches publiques dès lors qu'elles traitent des informations classifiées du canton ou ont accès aux moyens informatiques du canton. Toutefois, les communes et les autres organisations chargées de tâches publiques ne tomberont pas sous le coup de cette loi si elles peuvent garantir une sécurité de l'information comparable. C'est le cas lorsque le respect de la norme minimale de la Confédération pour les TIC peut être garanti.

b) **Bâle-Campagne :** le canton entend réviser entièrement ses dispositions de sécurité pour pouvoir mettre en œuvre la LSI. S'il ne prévoit pas, à ce jour, d'édicter une législation cantonale spécifique, il entreprend actuellement la révision des ordonnances sur l'informatique et la sécurité de l'information et des directives internes sur la sécurité de l'information.

c) **Saint-Gall :** les chancelières et chanceliers des cantons de Suisse orientale ont échangé sur les mesures à prendre en vue de mettre en œuvre la LSI. Ils ont rédigé un courrier commun daté du 15 octobre 2024 à l'attention du Secrétariat d'État à la politique de sécurité de la Confédération (SEPOS), dans lequel ils demandant à la Confédération de coordonner la mise en œuvre de la LSI et d'apporter un soutien adéquat, par exemple sous la forme d'un guide, ainsi que, en ce qui concerne la législation, de rédiger un modèle d'acte législatif qui s'alignerait par exemple sur la LSIC bernoise.

d) **Zoug :** la procédure législative dédiée à la mise en œuvre de la LSI fait encore l'objet d'une clarification juridique à l'automne 2024. Il est question d'élaborer une loi ou une ordonnance, que le Conseil d'État pourrait édicter sur la base de ses compétences constitutionnelles.

e) **Zurich :** le canton prévoit de mettre en œuvre la LSI pour l'administration cantonale au moyen d'une directive du Conseil-exécutif, la *Allgemeine Informationssicherheitsrichtlinie (AISR)* (« directive générale sur la sécurité de l'information »), qui posera les bases du système cantonal de gestion de la sécurité de l'information (Information Security Management System, ISMS). Une procédure de co-rapport interne est en cours à l'automne 2024. En principe, l'AISR porte uniquement sur l'administration cantonale (pouvoir exécutif), mais elle est également applicable à toutes les autres autorités qui utilisent des systèmes cantonaux ou traitent des informations du canton.

2.2 Collaboration du ou des cantons avec le nouveau SEPOS et l'ANS

Quel est le rôle du SEPOS ?

Les tâches du SEPOS sont définies à l'article 7 de l'ordonnance sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS, RS 172.214.1). Pour ce qui concerne le présent contexte, le SEPOS veille à la sécurité du traitement des informations pour lesquelles la Confédération est compétente (al. 1, lit. *c*) et il conduit les services spécialisés chargés de la sécurité de l'information, des contrôles de sécurité relatifs aux personnes et de la procédure de sécurité relative aux entreprises (al. 2).

La collaboration du SEPOS avec les cantons est régie par la loi fédérale sur la sécurité de l'information (LSI, RS 232). Cette loi prévoit l'existence d'une Conférence des préposés à la sécurité de l'information de la Confédération, à laquelle participent également deux personnes représentant les cantons (art. 82, al. 1 LSI), qui veille à l'échange d'informations et assure la coordination dans le domaine de la sécurité de l'information (al. 2). La Conférence joue un rôle de conseil pour les nouveaux projets planifiés par la Confédération, dont la faisabilité pour les cantons est évaluée par les représentantes ou représentants de ceux-ci. En outre, le service spécialisé de la Confédération chargé de la sécurité de l'information a pour mission au SEPOS de conseiller les cantons dans l'exécution de la LSI (art. 83, al. 1, lit. *a* LSI). Il donnera aux cantons notamment l'accès aux bases de formation et aux directives de la Confédération.

En outre, l'article 86, al. 4 LSI prévoit que le Conseil fédéral définit les cas dans lesquels les cantons peuvent, contre paiement d'un émolument, recourir aux prestations des services spécialisés au sens de la LSI afin d'assurer leur propre sécurité de l'information. Les cantons peuvent dans ce cadre, sur la base d'une convention de prestations passée avec le DDPS, demander au service spécialisé chargé de mener la procédure de sécurité relative aux entreprises de procéder à un contrôle de sécurité de leurs mandataires (art. 24 de l'ordonnance sur la procédure de sécurité relative aux entreprises, OPSEnt, RS 128.41). Il s'agit de déterminer si une entreprise est apte à exécuter un mandat sensible sur le plan de la sécurité ou s'il existe un risque pour la sécurité (art. 55 ss LSI). Les cantons peuvent de même recourir pour leur propre sécurité de l'information, contre paiement d'un émolument, aux prestations du service spécialisé chargé des contrôles de sécurité relatifs aux personnes lorsqu'ils disposent d'une base légale suffisante pour les contrôles à effectuer en vertu de l'OCSP, lorsqu'ils entendent effectuer des évaluations à l'instar de la Confédération pour garantir la sécurité de l'information, et lorsqu'ils ont conclu une convention de prestations avec le DDPS (art. 35 de l'ordonnance sur les contrôles de sécurité relatifs aux personnes, OCSP, RS 128.31).

Quelles tâches incombent / n'incombent pas à l'ANS ?

L'Administration numérique suisse (ANS) est une organisation commune de la Confédération et des cantons. Elle a pour mission d'encourager la transformation numérique des administrations en Suisse, en particulier par le développement de normes et en tant que plateforme politique. Pour ce faire, elle promeut le partage et la coordination des projets de transformation numérique de l'administration menés à l'échelon fédéral et intercantonal, émet des recommandations, collabore avec d'autres organisations spécialisées et recherche le dialogue avec le monde scientifique, le monde économique et la société civile. Les entités qui en assument la responsabilité entendent la développer de sorte à en faire une plateforme politique habilitée à fixer des normes contraignantes (ch. 2 de la convention-cadre de droit public concernant l'Administration numérique suisse, FF 2021 3030).

La convention-cadre n'attribue pas explicitement de tâches dans le domaine de la sécurité de l'information et de la cybersécurité à l'ANS. Cependant, il incombe notamment à celle-ci de promouvoir le développement de bases juridiques et politiques communes et la définition d'un cadre commun pour l'admi-

nistration numérique, mais aussi de renforcer la mise en réseau, la collaboration et les échanges de connaissances au sein des administrations aux trois niveaux de l'État (ch. 4.2, lit. *d* et *f* de la convention-cadre). La Direction des finances estime par conséquent qu'il revient également à l'ANS de coordonner et de soutenir la création des bases légales cantonales dédiées à la sécurité de l'information. En effet, la sécurité est l'un des piliers de la numérisation et la collaboration que l'ANS doit promouvoir en matière de numérisation suppose que les collectivités qui coopèrent harmonisent leurs prescriptions et mesures de sécurité.

C'est donc à juste titre que la CIRE a exigé, dans le cadre des délibérations de la LSIC, que la Direction des finances demande à l'ANS de coordonner les activités législatives des cantons et de la Confédération dans le domaine de la sécurité de l'information et de la cybersécurité. Néanmoins, cette démarche est malheureusement restée infructueuse :

Le responsable de l'ANS (chargé de mission de la Confédération et des cantons auprès de l'Administration numérique suisse) n'a pas réagi aux deux demandes qui lui ont été soumises le 30 octobre 2023 et le 6 décembre 2023. À la suite d'un nouveau courrier adressé le 19 janvier 2024 à l'ANS par la Directrice des finances, une rencontre a eu lieu le 30 janvier 2024 entre des personnes représentant la Direction des finances et l'ANS. Par courrier du 9 février 2024 à l'attention de la Direction des finances, le chargé de mission a résumé comme suit les conclusions qui en ont été tirées : « Le Secrétariat de l'ANS organisera bientôt, en coordination avec les activités du SEPOS, une table ronde avec des personnes représentant la Confédération et les cantons afin de clarifier si les cantons sont intéressés par une coordination et quelle forme celle-ci prendrait. Sur cette base, l'ANS réfléchira à la mise en place d'un groupe de travail, d'un projet ou d'une autre structure appropriée pour coordonner les exigences et les axes de la législation en matière de sécurité de l'information et des dispositions d'exécution y afférentes ».

L'ANS n'a toutefois pas mis en œuvre cet accord. Le 7 juin 2024, l'ANS a informé l'OIO que la Conférence des préposés à la sécurité de l'information de la Confédération s'était tenue le 5 juin 2024 avec trois personnes représentant les cantons et que le SEPOS avait planifié une conférence en septembre 2024, à laquelle il était prévu que tous les cantons participent. L'ANS a constaté que la coordination des activités législatives était principalement conduite par le SEPOS. Elle a estimé que les structures établies et les structures planifiées répondaient aux attentes du canton de Berne. La conférence du SEPOS mentionnée est désormais prévue pour novembre 2024.

Pour la suite des travaux, la Direction des finances se concentre donc sur les échanges directs avec le SEPOS et les responsables de la sécurité d'autres cantons (voir ci-dessus).

2.3 Interpellation 050-2024 « Collaboration entre le canton et les communes en matière de numérisation » (2024.RRGR.70)

Quelle conclusion peut-on tirer, pour la LSIC et sa mise en œuvre, de la réponse à l'intervention ? L'étude mentionnée peut-elle être mise à la disposition du Grand Conseil ou au moins de la CIRE ?

La Direction des finances répond à cette question en concertation avec le Secrétariat à l'administration numérique de la Chancellerie d'État.

L'interpellation 050-2024 a soulevé des questions sur la collaboration entre le canton et les communes en matière de numérisation. Dans sa réponse du 4 septembre 2024, le Conseil-exécutif a reconnu que des changements étaient nécessaires pour améliorer la collaboration et a informé que le canton avait commandé, en collaboration avec l'Association des Communes Bernoises (ACB), une étude censée fournir des propositions concrètes. Les premiers résultats de l'étude sont désormais disponibles. La

Chancellerie d'État, responsable du dossier pour le canton, va maintenant rédiger un rapport d'appréciation à l'intention du Conseil-exécutif, qui décidera de la suite de la procédure. Dès que ces travaux seront achevés, l'étude et le rapport d'appréciation pourront être remis à la CIRE.

L'interpellation n'aborde pas les questions de sécurité de l'information et de cybersécurité. C'est pourquoi l'étude ne porte pas non plus sur ce sujet en particulier. Cependant, nous considérons que les bases et structures organisationnelles et juridiques qui devront éventuellement être créées afin d'approfondir la collaboration entre le canton et les communes en matière de numérisation se prêteront également à l'organisation et à l'amélioration de la collaboration dans le domaine de la sécurité de l'information et de la cybersécurité, étroitement lié à la numérisation, pour autant que le besoin s'en fasse ressentir. La Chancellerie d'État et la Direction des finances tiendront compte de cet aspect dans la suite des travaux.

2.4 Champ d'application de la loi pour les communes et conséquences de la loi sur celles-ci

La CIRE estime qu'il existe certaines incohérences et contradictions concernant le champ d'application de la loi et ses répercussions sur les communes.

Conformément à l'article 2, la loi s'applique aux communes sous réserve uniquement :

Art. 2

Champ d'application

[1] La présente loi s'applique aux autorités cantonales et aux communes au sens de la Constitution cantonale (titres 5 et 7), sous réserve de l'alinéa 2.

[2] Ne s'appliquent aux autres organisations chargées de tâches publiques et aux communes que les dispositions sur

a les informations classifiées, lorsqu'elles traitent des informations classifiées du canton ou de la Confédération,

b la sécurité de l'utilisation d'outils TIC, lorsqu'elles se servent d'outils TIC du canton ou de la Confédération.

Le rapport donne les explications suivantes à ce sujet : « en vertu du principe de subsidiarité, elle ne s'applique aux communes et aux autres autorités autonomes au plan de l'organisation (hôpitaux, hautes écoles, entreprises publiques bernoises, etc.) que lorsque celles-ci utilisent des informations ou interagissent avec des systèmes du canton ou de la Confédération. Pour le reste, il leur incombe de se doter de dispositions de sécurité adaptées à la protection que nécessitent leurs informations. En vertu de l'article 17 LCPD, elles sont en outre tenues de sécuriser les données personnelles (cf. commentaire de l'art. 3 ci-dessous) ».

Dans le même temps, le rapport contient notamment les déclarations suivantes :

- *Chiffre 2.2, page 4 : « Par ailleurs, comme toutes les autorités cantonales et communales du canton de Berne sont interconnectées via des outils TIC, la sécurité de l'information et la cybersécurité ne peuvent être garanties que grâce à des règles valant pour toutes les autorités. C'est le rôle de la LSIC ».*
- *Chiffre 3.2.1, page 7 : « Le canton de Berne ne dispose donc pas non plus d'une organisation de la sécurité efficace et limitant les coûts ».*

- *Chiffre 8.4.1, page 21 : « La LSIC fixe sur le principe les tâches que l'autorité mandante doit accomplir pour assumer ses responsabilités en matière de sécurité (cf. art. 5 Obligation des autorités). Le Conseil-exécutif doit les définir plus précisément dans une procédure de sécurité standardisée valable pour l'ensemble des autorités. […] Les principales étapes de la procédure doivent être harmonisées par voie d'ordonnance pour toutes les autorités, pas seulement pour celles de l'administration cantonale ».*

Par conséquent, dans un contexte global, la CIRE est d'avis qu'il en résulte pour les communes une véritable obligation de se doter d'une organisation de la sécurité globale conforme aux exigences cantonales, dont le périmètre dépasse explicitement les informations et les systèmes du canton ou de la Confédération. Il convient à cet égard de se référer également aux commentaires de l'article 29, qui, selon le rapport, s'applique également aux communes. La Direction des finances a toutefois indiqué dans le cadre de la séance de la Commission que cette disposition ne s'appliquait pas aux communes.

La CIRE s'attend quoi qu'il en soit à ce que la LSIC ait de vastes répercussions sur les communes, ce qui posera des difficultés majeures, notamment financières, aux petites communes.

Par conséquent, la CIRE aimerait clarifier le point suivant : quelles sont exactement les dispositions qui s'appliquent aux communes ?

Le **champ d'application de la LSIC** repose sur le principe suivant : la loi est contraignante pour les communes et les autres organisations chargées de tâches publiques (OCTP) uniquement dans la mesure où cela est nécessaire pour préserver les intérêts de la Confédération et du canton en matière de sécurité, c'est-à-dire uniquement dans la mesure où cela est nécessaire pour protéger les informations ou les systèmes TIC de la Confédération ou du canton. Cela correspond à la teneur de l'article 3 LSI, selon lequel la loi s'applique aux cantons uniquement dans la mesure où les informations ou les systèmes de la Confédération sont concernés. De plus, cela reflète l'autonomie d'organisation des communes et des OCTP : Étant donné que la LSIC concerne « uniquement » les intérêts de sécurité des autorités et non ceux de la population (voir ci-après), il n'est pas nécessaire que le canton prescrive aux communes et aux OCTP la manière dont celles-ci doivent protéger leurs propres intérêts en matière de sécurité. Cependant, le canton estime judicieux que les communes et les OCTP se conforment elles aussi à la LSIC, le cas échéant en pratiquant certains ajustements qui reflètent les risques auxquelles elles sont exposées, comme le fait le canton avec la LSI.

Notons par ailleurs que la LSIC, à l'instar de la LSI, limite doublement son champ d'application puisqu'elle s'applique uniquement dans le domaine de la collaboration avec les niveaux supérieurs de l'État et uniquement en ce qui concerne les règles relatives aux informations classifiées et à la sécurité des outils TIC.

Pour ce qui est de la **révision totale prévue de la loi sur la protection des données (LCPD)**, il convient toutefois d'émettre une réserve importante par rapport à ce qui précède. Comme susmentionné, la LSIC règle exclusivement la sécurité des informations dont la protection est nécessaire à la sauvegarde d'intérêts publics ; elle ne porte pas sur la protection, tout aussi importante, des données personnelles, c'est-à-dire des informations dont la protection est nécessaire à la sauvegarde de la sphère privée des individus. Cette question relève du droit de la protection des données. Pour ces deux catégories d'informations, les méthodes de protection sont toutefois les mêmes pour autant que l'on considère les objectifs de protection de la sécurité (confidentialité, disponibilité, intégrité et traçabilité).

C'est pourquoi le projet de révision totale de la LCPD prévoit que les *principes* de la LSIC s'appliquent également par analogie à la sécurité des données personnelles (dite sécurité des données). La Direction des finances et la Direction de l'intérieur et de la justice préparent donc une ordonnance d'exécution

commune pour ces deux nouvelles lois, l'ordonnance sur la sécurité de l'information et des données (OSID). Ces actes législatifs ainsi que les dispositions d'exécution correspondantes règleront de manière uniforme les méthodes visant la sécurité des informations étatiques et des données personnelles. Par ailleurs, étant donné que la LCPD s'applique et continuera de s'appliquer également sans restriction (contrairement à la LSIC) aux communes et aux OCTP, les dispositions d'exécution communes aux deux lois s'appliqueront aussi intégralement aux communes et aux OCTP pour ce qui concerne la sécurité des données. Cela ne constitue pas une nouveauté puisque, aujourd'hui déjà, l'ordonnance sur la protection des données (OPD, RSB 152.040.1) prescrit aux articles 4 à 9 à toutes les autorités, y compris aux communes et aux OCTP, les mesures à prendre pour garantir la sécurité des données. Ces thèmes à réglementer seront repris dans l'OSID et adaptés à l'état actuel de la technique, mais le Grand Conseil pourra décider ultérieurement, lors des délibérations de la révision totale de la LCPD, s'il consent à cette solution.

Par conséquent, la question de savoir dans quelle mesure la LSIC et ses dispositions d'exécution s'appliquent aux communes et aux OCTP appelle deux réponses séparées, selon que l'on considère la période avant ou après la révision totale planifiée de la LCPD (rLCPD) :

Partie LSIC	LSIC uniquement	LSIC et rLCPD	Remarques
1 Dispositions générales	✓ **S'applique**	✓ **S'applique**	Ne contient aucune obligation.
2 Principes	✗ **Ne s'applique pas**	✓ **S'applique (DP)**	Selon la rLCPD, les principes de la LSIC doivent également s'appliquer par analogie aux données personnelles.
3 Mesures concernant l'organisation	○ **S'applique en partie**	○ **S'applique en partie**	Seules les règles relatives au traitement des informations classifiées des niveaux supérieurs de l'État sont applicables.
4 Mesures techniques	○ **S'applique en partie**	○ **S'applique en partie**	*LSIC uniquement :* les règles prescrites par le niveau supérieur de l'État concernant l'utilisation des outils TIC de celui-ci, le cas échéant la procédure de sécurité relative au traitement des informations classifiées de la Confédération ou du canton (voir ci-dessous), s'appliquent. *Avec rLCPD :* les dispositions d'exécution communes relatives à la LSIC et à la rLCPD peuvent entraîner l'application de la procédure de sécurité relative au traitement des données personnelles.
5 Mesures physiques	✗ **Ne s'applique pas**	✗ **Ne s'applique pas**	–
6.1 Sélection, formation et habilitation	○ **S'applique en partie**	○ **S'applique en partie**	*LSIC uniquement :* seules les règles relatives à l'utilisation des outils TIC prescrites par le niveau supérieur de l'État sont applicables.

Partie LSIC	LSIC uniquement	LSIC et rLCPD	Remarques
			Avec rLCPD : les dispositions d'exécution communes à la LSIC et à la LCPD peuvent entraîner l'application de ces principes au traitement des données personnelles.
6.2 Contrôle de sécurité relatif aux personnes	✘ **Ne s'applique pas**	✘ **Ne s'applique pas**	Si les communes souhaitent réaliser un CSP, elles doivent en fixer elles-mêmes les modalités par règlement, par exemple au moyen d'un renvoi à la LSIC.
7 Organisation de la sécurité	✘ **Ne s'applique pas**	✘ **Ne s'applique pas**	L'article 29 concerne uniquement les autorités cantonales qui sont pleinement soumises à la loi mais ne font pas partie de l'administration (p. ex. la Justice).
8 Dispositions d'exécution	○ **S'applique en partie**	○ **S'applique en partie**	*LSIC uniquement :* seules les dispositions d'exécution relatives à l'utilisation des outils TIC et des informations classifiées des niveaux supérieurs de l'État sont applicables. *Avec la rLCPD :* au surplus, les dispositions d'exécution communes à la LSIC et à la rLCPD en matière de sécurité des données personnelles sont applicables.

Dans ce contexte, les passages du rapport cités ci-dessus par la CIRE sont potentiellement ambigus et doivent être explicités ou précisés ici :

1. Le passage tiré du chiffre 2.2, page 4 du rapport est pertinent car il reflète la nécessité d'appliquer des règles uniformes dans le domaine de la collaboration entre les différents niveaux étatiques, comme le prévoit la LSIC.

2. Au chiffre 3.2.1, page 7 du rapport, le « canton de Berne » désigne la collectivité territoriale et son administration cantonale, et non l'ensemble des autorités présentes sur le territoire cantonal, bien que l'affirmation s'appliquerait probablement aussi à de nombreuses communes et OCTP.

3. Toutefois, lorsqu'il est question, au chiffre 8.4.1, page 21 du rapport, de la nécessité d'harmoniser les étapes de la procédure de sécurité « pour toutes les autorités, pas seulement pour celles de l'administration cantonale », cela n'est que partiellement exact, du moins selon la perspective de la LSIC : étant donné que, en vertu de l'article 2, les communes et les OCTP ne sont soumises à la LSIC que lorsqu'elles utilisent des systèmes ou traitent des informations de la Confédération ou du canton, les dispositions relatives à la procédure de sécurité ne sont applicables aux communes et aux OCTP que dans ces mêmes conditions. Cela signifie qu'une procédure de sécurité conforme aux directives cantonales est requise pour les systèmes des communes uniquement si les communes souhaitent traiter des informations classifiées du canton dans de tels systèmes propres, ce qui sera sans doute rarement le cas.
   Cependant, comme mentionné ci-avant, il est prévu que la LCPD révisée entraîne l'application des directives de sécurité cantonales également au traitement de données personnelles par les communes. Si le Grand Conseil approuve cette approche dans le cadre de la révision de la LCPD, il est possible que les communes soient contraintes d'appliquer une procédure de sécurité également pour

les systèmes avec lesquelles elles souhaitent traiter des données personnelles sensibles. Il conviendra de déterminer lors des travaux d'élaboration des dispositions d'exécution, notamment en concertation avec les personnes représentant les communes, dans quels cas cela est proportionné.

Quelles sont les obligations « implicites », pour les communes, qui découlent de la loi (conformément au principe « Une chaîne n'est jamais plus solide que son maillon le plus faible ») ?

Ce principe s'applique à la collaboration des communes avec la Confédération et le canton, c'est-à-dire dès lors que les communes utilisent des systèmes ou traitent des informations de la Confédération ou du canton. Il est alors important que l'ensemble des parties prenantes assurent le même niveau de sécurité, autrement dit, qu'elles appliquent les dispositions de sécurité définies dans la LSIC ou les conditions d'utilisation imposées par le niveau supérieur de l'État. En outre, il est prévu dans le cadre de la révision susmentionnée de la LCPD que les dispositions de sécurité cantonales s'appliquent également au traitement de données personnelles, étant donné qu'il importe peu pour les citoyennes et citoyens, dont il convient de protéger la sphère privée, que les données personnelles soient traitées par une commune ou par le canton.

Comment les autres autorités, outre les communes, sont-elles soutenues dans la mise en place de l'organisation de la sécurité et dans l'habilitation en la matière, à quelles conditions peuvent-elles bénéficier d'une assistance par le canton et quelles ressources seraient pour cela requises par le canton (voir aussi ci-dessous « Coûts/ressources ») ? En effet, les FAQ sont insuffisantes pour les communes. Elles ont besoin de modèles et d'un support concrets.

L'OIO soutient comme suit les autorités cantonales et communales dans la mise en œuvre de la LSIC :

1. Premièrement, il va mettre à la disposition de toutes les autorités, sur Internet, les **modèles, outils d'aide et supports de formation** élaborés dans le cadre du projet IS@BE. Cela comprend entre autres des modèles et des documents types pour la documentation de sécurité. Le canton propose également des offres de formation initiale et continue à bas seuil pour les collaboratrices et collaborateurs et les spécialistes TIC, notamment des séminaires en ligne (visioconférences avec la possibilité de poser des questions en direct et de visionner l'enregistrement ultérieurement) et des séquences de formation en ligne (séquences interactives avec exercices et tests).

2. Deuxièmement, l'OIO soutient les autorités cantonales et communales dans le cadre de ses possibilités en leur fournissant des **conseils** sur la procédure appropriée en matière de sécurité de l'information. L'une des approches pour cela consiste à donner la possibilité aux responsables de la sécurité des communes d'entrer facilement en contact avec les spécialistes de la sécurité du canton, afin d'obtenir une réponse rapide à leurs questions et requêtes simples.

3. Néanmoins, les ressources en personnel du canton étant insuffisantes pour apporter des conseils ou un soutien approfondis aux autorités cantonales et communales, l'OIO permet – troisièmement – temps à toutes les autorités et à toutes les organisations chargées de tâches publiques dans le canton de **recourir à des prestations de sécurité auprès de prestataires externes.** En 2023, l'OIO a déjà mis au concours un contrat-cadre correspondant en faveur de toutes les autorités. Il comprend les prestations suivantes :
   a) *Spécialiste de la sécurité des TIC Junior, Senior, Senior Expert :* conseiller et soutenir les cadres et les collaboratrices et collaborateurs dans l'élaboration de documents SIPD sur la base des modèles existants (concept SIPD, analyses des risques, etc.) et dans la mise en œuvre des mesures qui en découlent. Assumer le rôle HERMES en tant que responsable SIPD. Participer à l'élaboration des directives en matière de sécurité de l'information à tous les niveaux. Vérifier le respect des consignes de sécurité. Sensibiliser à la sécurité de l'information et la protection des données au sein des unités administratives.

b) *Chargé·e de la sécurité des TIC Senior :* apporter un soutien et des conseils pour les tâches de conception dans le domaine ISMS. Participer à l'élaboration des directives en matière de sécurité de l'information à tous les niveaux. Rechercher des informations en cas de questions complexes liées à la sécurité. Vérifier le respect des consignes de sécurité.
c) *Sensibilisation à la sécurité informatique :* pour la sensibilisation des collaboratrices et collaborateurs, le partenaire du contrat-cadre utilise un outil qui contient déjà des contenus standardisés (campagnes, formations en ligne). Il dispose en outre d'un plan d'action et est en mesure de réaliser des évaluations. Il propose les rôles de chef·fe de projet / conseiller/ère en sensibilisation et de spécialiste en intégration, ingénierie sociale.
d) *Audit de sécurité informatique :* l'audit comprend une analyse de la sécurité et des risques sur la base des vulnérabilités et des failles de sécurité existantes, des processus ou des mesures organisationnelles dans une organisation, ainsi que l'élaboration de propositions de mesures. Le partenaire du contrat-cadre propose les rôles de responsable d'audit et de chargé·e d'audit.
e) *Tests d'intrusion informatique :* un test d'intrusion informatique permet de vérifier, par exemple dans le cadre d'un audit de sécurité informatique, la sécurité du plus grand nombre possible de composants du système et d'applications d'un réseau ou d'un système logiciel au moyen d'outils et de méthodes qui permettent potentiellement un accès non autorisé au système (intrusion). Le prestataire s'appuie sur une procédure standardisée (p. ex. OSSTMM) pour réaliser les tests d'intrusion informatique.

Cet appel d'offres groupé pour l'ensemble du canton permet aux autorités bernoises de bénéficier de conditions plus avantageuses que si chacune acquérait ses propres prestations. Les conditions sont soumises à l'obligation contractuelle de garder le secret et sont communiquées aux autorités intéressées sur demande. Cette offre ainsi que d'autres offres d'achat centrales du canton sont consultables actuellement sur l'intranet du canton (en allemand uniquement), auquel les communes et les membres du Grand Conseil ont accès via le poste de travail cantonal. À partir de décembre 2024, ces offres seront publiées sur Internet (www.be.ch/marchespublics> Centrales d'achat cantonales (CAC) > CAC TIC).

S'il s'avère lors de la mise en œuvre que le volume des prestations ou les capacités des partenaires du contrat-cadre ne suffisent pas à répondre à la demande, l'OIO est disposé à concevoir et à lancer, en collaboration par exemple avec des personnes représentant l'ACB et les OCTP de grande taille, un appel d'offres public complémentaire.

4. Enfin, quatrièmement, l'OIO a l'intention de concevoir et de mettre en œuvre, avec le soutien des partenaires du contrat-cadre des prestations susmentionnées, une **formation initiale ou continue pour les responsables de la sécurité et les collaboratrices et collaborateurs des communes** afin de remplir le mandat qui, selon la volonté de la CIRE, doit être inscrit à l'article 19, alinéa 2 LSIC. Le contenu et la durée de cette formation initiale ou continue seront également définis en collaboration avec les représentantes et représentants de communes et d'OCTP intéressées et avec l'ACB et/ou l'association Cadres des communes bernoises.

2.5 Coûts/ressources

Selon le rapport, la mise en œuvre de la loi ne doit pas générer de coûts supplémentaires (ch. 10 et 11). La CIRE reste sceptique sur ce point. L'affirmation « Le canton de Berne ne dispose donc pas non plus d'une organisation de la sécurité efficace et limitant les coûts » va d'ailleurs dans ce sens. À lui seul, l'engagement de personnel doté des compétences requises pour la mise en œuvre de l'organisation de la sécurité dans l'administration cantonale va engendrer des coûts supplémentaires (voir les dispositions relatives aux compétences dans le projet d'ordonnance, art. 38, al. 4). La Direction des finances a elle-

même reconnu dans les questions et réponses qu'il n'était pas possible de chiffrer les gains d'efficience que la numérisation dégagera.

Par conséquent, la CIRE souhaite obtenir des explications sur les domaines dans lesquels la Direction des finances identifie de manière réaliste des besoins en ressources supplémentaires.

Il va de soi que l'administration publique devra à l'avenir consacrer davantage de moyens financiers et engager davantage de personnel en faveur de la sécurité de l'information et de la cybersécurité. Toutefois, cette charge supplémentaire ne résulte pas de la LSIC en tant que telle, car la loi et ses dispositions d'exécution décrivent uniquement ce qui constitue à ce jour « l'état de l'art » de la sécurité de l'information. Ainsi, la législation ne fait que refléter ce que les autorités doivent ou devraient en principe déjà entreprendre à ce jour afin de se prémunir contre les accès non autorisés aux informations et de protéger contre les cyberattaques leurs systèmes ainsi que leur capacité à accomplir leurs tâches.

La charge supplémentaire découle en réalité des risques de sécurité en forte augmentation, qui existent indépendamment de la LSIC. Ces risques sont d'une part liés à la vulnérabilité croissante de l'économie, de la société et de l'administration publique de Suisse face aux cyberrisques. À mesure que la numérisation s'étend à tous les domaines de la vie, il est devenu, en quelques années seulement, beaucoup plus probable que des cyberattaques contre des infrastructures essentielles paralysent dans une large mesure la vie publique et économique en Suisse, ou qu'un grand nombre de personnes se retrouvent atteintes dans leur sphère privée suite au vol de grandes quantités de données ou dans leur patrimoine à cause d'une usurpation d'identité. Par ailleurs, les risques de sécurité croissants ne résultent pas non plus de l'augmentation des tensions géopolitiques et des conflits armés, qui, de plus en plus, s'étendent au cyberespace et touchent directement la Suisse. Ainsi la conseillère fédérale Viola Amherd a-t-elle écrit en préface du rapport sur la sécurité 2024 du Service de renseignement de la Confédération (SRC) : « La Russie et d'autres acteurs étatiques mènent [...] un conflit hybride contre les États occidentaux. Celui-ci nous concerne directement, sous la forme d'activités d'espionnage, de prolifération et d'influence ».

Pour contrer ces risques croissants, il est indispensable que les autorités du canton de Berne prennent davantage de mesures concrètes au cours des années à venir dans les domaines suivants, si elles ne l'ont pas déjà fait :

1. La **mise en œuvre de mesures de sécurité.** Il s'agit par exemple
   a) de protéger efficacement les informations sensibles contre les accès non autorisés (p. ex. par cryptage) à chaque étape de leur traitement,
   b) de mettre en place et de maintenir un système de gestion des personnes autorisées à accéder aux informations sensibles et de leurs droits d'accès (« Identity and Access Management »), qui garantit notamment que chaque personne, à tout moment, ne dispose pas plus d'autorisations que nécessaire.
   c) d'assurer une authentification sûre des utilisateurs lors de leur connexion aux systèmes informatiques, qui exclut autant que possible que des personnes non autorisées puissent se faire passer pour des personnes autorisées, par exemple au moyen d'une méthode d'authentification à deux facteurs, qui requiert un mot de passe ainsi qu'un autre élément d'accès tel qu'un code issu d'une application sur smartphone, et
   d) de contrôler régulièrement la fiabilité des personnes ayant accès à des informations sensibles au moyen d'un contrôle de sécurité des personnes.

2. Les mesures qui permettent d'**aménager les mesures de sécurité en fonction des risques,** par exemple :
   a) la mise en place et la maintenance d'un système de gestion des risques permettant à la direction d'identifier et d'évaluer régulièrement les risques de sécurité et de les éviter ou les réduire au moyen de mesures ou alors de les accepter, ainsi que

b) la classification de toutes les informations et de tous les outils TIC en fonction de leur besoin de protection, afin de pouvoir adapter les mesures de sécurité au besoin de protection et ainsi d'éviter les mesures de sécurité excessives ou trop coûteuses.

3. Le **contrôle régulier de la mise en œuvre des mesures de sécurité** par toutes les parties prenantes telles que les fournisseurs de prestations externes (en cas de traitement de données sur mandat), les organisations partenaires ayant accès aux informations internes et les collaboratrices et collaborateurs internes. Cela passe par exemple par
   a) la demande et l'évaluation d'un rapport sur la mise en œuvre des mesures,
   b) des audits de la documentation de sécurité et des systèmes informatiques,
   c) l'évaluation des rapports d'incidents de sécurité éventuels et des contre-mesures et
   d) le contrôle de l'efficacité des mesures de sécurité, par exemple en simulant des attaques sur sa propre organisation et ses propres systèmes afin de repérer les vulnérabilités (tests d'intrusion).

4. Une organisation qui permet une **amélioration constante du niveau et de la culture de la sécurité** de l'autorité concernée, notamment
   a) un système de gestion de la sécurité de l'information (ISMS), composé des processus par lesquels une autorité définit ses exigences et objectifs en matière de sécurité, en déduit les mesures à prendre, les met en œuvre et contrôle leur application, dans le cadre d'un cycle « plan-do-check-act » qui se répète en permanence et conduit ainsi à une amélioration constante,
   b) une procédure permettant de signaler, suivre et évaluer simplement et rapidement les incidents de sécurité, mais aussi
   c) la formation et le perfectionnement des collaboratrices et collaborateurs internes pour les questions de sécurité, de manière adaptée à la fonction occupée, ainsi qu'un travail de sensibilisation régulière du personnel, par exemple au travers d'exercices permettant de contrôler si les collaboratrices et collaborateurs réagissent correctement face à des attaques simulées (p. ex. hameçonnage par courriel).

Pour ce faire, les autorités ont besoin de ressources adéquates. Cela vaut en principe aussi pour les communes et les OCTP. Néanmoins, les mesures doivent toujours être fixées et mises en œuvre en fonction des risques encourus. Il peut donc arriver que les communes constatent, après avoir évalué les risques, qu'une grande partie de ces mesures n'est pas ou pas entièrement nécessaire à leur niveau. De plus, l'expérience montre qu'il est plus simple et plus efficace de mettre en œuvre des mesures par petites étapes en visant une amélioration constante, plutôt que de chercher à améliorer brusquement le niveau de sécurité d'une organisation par le biais d'un projet d'envergure. Cela permet également d'échelonner les mesures dans le temps et de mettre en place progressivement des ressources supplémentaires dédiées à la sécurité.

Au vu de la situation financière du canton, il est inenvisageable de contrer la charge financière supplémentaire qui lui incombe en augmentant les dépenses ou le plafond de postes de l'administration. Le Conseil-exécutif entend donc compenser la charge supplémentaire dans l'administration cantonale dans le cadre du budget informatique en cours et planifié et des effectifs actuels. Il s'appuie pour cela sur trois approches :

1. Il souhaite mettre à profit les **gains d'efficience dégagés par la numérisation** pour investir dans la sécurité, ce qui suppose une exécution systématique par les autorités du mandat de la loi sur l'administration numérique pour numériser les processus. Plus les processus de travail seront numérisés et ainsi partiellement ou intégralement automatisés, notamment grâce à l'intelligence artificielle, plus les ressources en personnel s'en trouveront libérées pour le traitement des dossiers et pourront être affectées par exemple à des postes de spécialistes de la sécurité.

2. Il souhaite renforcer la **collaboration en lien avec la numérisation**. Avec l'augmentation des coûts de l'informatique et de la sécurité informatique, il est essentiel que les autorités utilisent le plus possible des solutions communes, à tous les niveaux étatiques et en incluant les communes et tous les autres acteurs du secteur public. Cela permet d'effectuer un seul investissement pour le développement d'une solution unique en faveur de la sécurité. Pour cela aussi, la mise en œuvre du mandat de collaboration de la LAN est importante.

3. La **LSIC elle-même** constitue d'ailleurs un facteur important pour endiguer la hausse des coûts liés à la sécurité. Elle offre en effet aux autorités cantonales un cadre unique en matière de sécurité, comprenant des normes et des modèles uniformes. Par exemple, les différentes autorités n'ont pas besoin de décider quelles mesures de base prendre et comment les mettre en œuvre, ce qui les allège d'ores et déjà d'une charge non négligeable. Elles peuvent ainsi se concentrer sur l'identification et la gestion de leurs risques spécifiques.

2.6 Contrôles de sécurité relatifs aux personnes (CSP)

À ce sujet, la CIRE souhaite obtenir des explications quant à la manière exacte dont le système prévu fonctionnera selon le projet du Conseil-exécutif, c'est-à-dire sans forme ou organe de contrôle uniforme, sans différenciation des niveaux de contrôle, sans périodicité et sans réglementation pour la conservation/destruction des données relevées. Il convient à cet égard de revenir sur les explications données oralement par la Direction des finances lors de la séance de la Commission, à savoir notamment que les contrôles de sécurité relatifs aux personnes devraient se limiter dans la grande majorité des cas à la demande d'extraits du casier judiciaire et du registre des poursuites et que ces contrôles concernent peu de fonctions de manière générale.

Compte tenu du fait que la CIRE a décidé à l'unanimité que les dispositions relatives au CSP devaient être renvoyées au Conseil-exécutif, la Direction des finances propose au Conseil-exécutif de se rallier à cette proposition. Il est prévu qu'une nouvelle proposition de réglementation soit ensuite délibérée en deuxième lecture. C'est pourquoi nous ne nous étendrons pas sur la proposition de réglementation du Conseil-exécutif, qui semble désormais vouée à l'échec.

Selon la conception du Conseil-exécutif que la CIRE propose de renvoyer, la procédure de contrôle de sécurité relatif aux personnes, déjà prévue dans la loi sur la police, doit être étendue à l'ensemble des autorités cantonales. Cela signifie que chaque autorité pourra décider elle-même des personnes à contrôler, mais pas pour autant que chaque collaboratrice ou collaborateur pourra à l'avenir être en quelque sorte « passé au crible » au gré des envies de sa ou son supérieur. En effet, l'article 22 LSIC réserve le CSP aux personnes appelées, dans le cadre de leur activité, à avoir « accès fréquemment ou à de nombreuses informations » classifiées CONFIDENTIEL ou SECRET ou à consulter de telles informations. Le nombre de personnes à contrôler dans l'administration devrait donc se limiter à quelques centaines. Il devrait s'agir en premier lieu de cadres et de collaboratrices et collaborateurs des secrétariat généraux et des offices assumant des tâches de sécurité (p. ex. poca, OSSM, OEJ, OIO) ainsi que de spécialistes informatiques dotés d'autorisations étendues leur permettant d'accéder à des informations sensibles. Les membres de l'équipe de support de l'OIO en font notamment partie, de même que les gestionnaires de service des applications telles que BE-GEVER ou GERES, qui servent au traitement d'informations sensibles.

De même, chaque autorité fixe elle-même la date et la fréquence des contrôles et décide quelles informations, parmi celles prévues par la loi, entrent dans le cadre des contrôles ; Néanmoins, ces décisions ne sont pas prises de façon arbitraire, mais résultent de l'évaluation individuelle des risques pour les intérêts de l'autorité à protéger en matière de sécurité. De la même manière qu'elle doit par exemple exa-

miner quelles mesures physiques ou organisationnelles doivent être prises pour protéger ses informations, l'autorité doit évaluer quelles personnes engagées ou nominées par ses soins représenteraient un risque considérable pour les intérêts publics à protéger par la LSIC si elles s'avéraient par exemple corrompues ou vulnérables au chantage. Nous considérons qu'un contrôle du casier judiciaire et du registre des poursuites est généralement suffisant car, dans la plupart des cas, ces registres reflètent les défauts de caractère graves portés à la connaissance des autorités. Par contre, pour les rares fonctions qui présentent un risque potentiel très élevé, il peut être proportionné de se référer aussi à des informations provenant des bases de données de la police ou de personnes qui ont été en contact avec la personne soumise au contrôle.

Contrairement à la réglementation de la Confédération, très formalisée et judiciarisée, les dispositions relatives à la procédure de contrôle sont par ailleurs minimalistes. De même, la conservation des documents n'est pas réglée dans la loi. Les règles correspondantes devraient être fixées par ordonnance, en conformité avec le principe de protection des données, selon lequel les données personnelles ne doivent être conservées que le temps nécessaire à leur utilisation.

L'inconvénient de cette approche réglementaire, par rapport à la réglementation fédérale très détaillée, est que le CSP peut être mis en œuvre différemment d'une autorité à l'autre et qu'il est plus difficile pour les personnes concernées de prévoir si et quand elles seront contrôlées. Du point de vue de la Direction des finances, cette solution présente cependant un avantage déterminant : celui d'avoir fait ses preuves à la poca et de pouvoir être mise en œuvre en autonomie par chaque autorité, sans être contraint d'engager un grand nombre de spécialistes CSP comme c'est le cas à la Confédération.

En outre, il faut répondre aux besoins des communes (« le maillon le plus faible de la chaîne », voir également ci-dessus).

Selon la conception de la LSIC, la loi ne s'applique aux communes que de manière très limitée, à savoir dans la mesure où des intérêts de sécurité du canton ou de la Confédération sont concernés (voir ch. 2.4 ci-dessus). Dans ce contexte, il aurait été envisageable d'appliquer également aux communes les dispositions relatives au CSP dès lors que le personnel des communes traite des informations classifiées du canton ou de la Confédération. Cela n'est pas prévu dans la LSIC pour les raisons suivantes :

a) La charge que représente la LSIC pour les communes doit être réduite au minimum nécessaire à la protection des intérêts de sécurité du canton et de la Confédération.
b) Le traitement par les communes d'informations classifiées des niveaux étatiques supérieurs est probablement l'exception plutôt que la règle.
c) Pour les services cantonaux responsables de la sécurité, il serait difficile de garder une vue d'ensemble des personnes devant être soumises au CSP au niveau des communes et de s'assurer que les contrôles ont été réalisés dans les règles de l'art.
d) Il est plus fréquent à l'échelle communale qu'à l'échelle cantonale que les affaires soient traitées par des membres des autorités élus par la population (membres du conseil communal, du parlement ou de commission). Or, pour ces personnes, un CSP n'est prévu ni par la LSI, ni par la LSIC.

Pour ces raisons et au vu des risques encourus, la Direction des finances estime défendable d'exclure les communes du champ d'application des dispositions relatives aux CSP. Toutefois, si la CIRE voyait un avantage à ce que les communes et les autres OCTP aient la possibilité d'appliquer les dispositions sur les CSP pour protéger leurs propres intérêts de sécurité, la Direction des finances ne verrait pas d'objection de principe à des demandes qui iraient dans ce sens.

La CIRE souhaite en outre obtenir des explications sur la position de la Direction des finances concernant l'avis des spécialistes selon lequel les dispositions ont encore besoin d'être « affinées ».

D’après nos souvenirs (les procès-verbaux de la Commission ne sont pas encore disponibles au moment où nous répondons aux présentes questions), l’expert qui a été interrogé par la CIRE a indiqué que les dispositions relatives au CSP étaient trop vagues dans la LSIC. Selon lui, elles ne permettent pas de déterminer précisément quelles informations sont demandées à quel moment. Les niveaux de contrôle fixés par la Confédération sont quant à eux plus clairs. Ils devraient figurer également dans la LSIC.

Cependant, d’après nos souvenirs, l’expert n’a pas expliqué pour quelles raisons, par exemple juridiques ou politiques, il jugeait utile de préciser la réglementation. Nous ne pouvons donc pas en dire plus sur son évaluation. Nous ne pouvons à ce sujet que renvoyer à notre évaluation ci-avant selon laquelle nous estimons judicieux de laisser l’autorité responsable décider de l’étendue du CSP en fonction de sa propre évaluation des risques. En outre, nous tenons à souligner que les règles relatives au CSP proposées par le Conseil-exécutif ont été élaborées de concert avec le préposé cantonal à la protection des données, ce qui indique en tous les cas qu’elles ne sont pas problématiques du point de vue des droits fondamentaux.