Rapport

Date de la séance du CE :	25 janvier 2023
Direction :	Finanzdirektion
N° d'affaire :	2020.KAIO.134
Classification :	Non classifié

Loi sur la sécurité de l'information et la cybersécurité LSIC

Sommaire

1. Synthèse

Avec la transformation numérique de l'administration, il est de plus en plus important de veiller à la sécurité de l'information et à la cybersécurité pour protéger les systèmes de l'administration contre la cybercriminalité, qui va croissante. Sur ce plan, l'administration cantonale manque toutefois de fondements techniques, organisationnels et légaux à de nombreux égards. La sécurité de l'information et la cybersécurité n'y sont réglementées qu'au coup par coup et par des textes qui se trouvent au bas de la hiérarchie des normes. En outre, la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI)[1], dont l'entrée en vigueur est prévue pour le 1er avril 2023, commande aux cantons de se doter d'une législation équivalente.

Le présent projet de loi sur la sécurité de l'information et la cybersécurité (LSIC), qui a été élaboré dans le cadre du projet cantonal sur la sécurité de l'information dans le canton de Berne (SI BE), vient combler ces lacunes. Il complète la législation sur les fichiers centralisés de données personnelles (LFDP)[2] et sur l'administration numérique (LAN)[3] ainsi que la loi, révisée, sur la protection des données (LCPD)[4]. Le Conseil-exécutif a jeté les bases de ces travaux législatifs dans son programme gouvernemental de législature de 2019 à 2022[5] et dans la Stratégie pour une administration numérique (SAN)[6]. En outre, le comité stratégique TIC (CST) de l'administration cantonale a arrêté la Stratégie sur la sécurité de l'information BE 2022-2025 (Stratégie SIBE)[7].

La LSIC doit se focaliser sur les risques, les besoins et les possibilités spécifiques au canton de Berne. Avec ses 24 articles, elle est beaucoup moins volumineuse que la LSI, qui en compte plus de 100. Elle ne s'applique aux communes et autres organisations autonomes chargées de tâches publiques que lorsque celles-ci traitent des informations classifiées par le canton ou par la Confédération ou qu'elles utilisent les outils informatiques de ceux-ci.

Parmi les principales nouveautés apportées par la LSIC figurent des règles organisant la haute direction en matière de prévention et régissant la classification d'informations et d'outils TIC ainsi que le contrôle de sécurité relatif aux personnes (CSP). Le projet confie aux organes cantonaux chargés de l'administration numérique et des TIC les hautes responsabilités en matière de coordination et de pilotage de la sécurité de l'information et de la cybersécurité.

La sécurité de l'information et la cybersécurité ne se limitent pas aux outils TIC. Elles englobent aussi des mesures de sécurité physique, en particulier portant sur les personnes, l'être humain représentant la plus grande source de risques pour la sécurité de l'information et la cybersécurité.

[1] FF 2020 9665 ; https://www.fedlex.admin.ch/eli/fga/2020/2696/fr
[2] LFDP, RSB 152.05 ; https://www.belex.sites.be.ch/app/fr/texts_of_law/152.05/versions/2140
[3] 2021.STA.1412 : LAN, documents pour la 2e lecture, session de printemps de 2022
[4] LCPD, RSB 152.04 ; https://www.belex.sites.be.ch/app/fr/texts_of_law/152.04/versions/2000
[5] ACE 1311/2018
[6] ACE 719/2019
[7] Stratégie SIBE : https://wwwin.kaio.fin.be.ch/intranet_kaio_fin/fr/index/das_kaio/das_kaio/weisungen/1_1_strategie.assetref/dam/documents/intranet_kaio_fin/das_kaio/fr/Weisungen/1_1_005_Strategie%20sur%20la%20securite%20de%20l_information%20BE%202022_2025.pdf

Il est prévu que la LSIC, comme l'ordonnance qui s'y rapporte, entre en vigueur dans le courant de l'année 2024.

2. Sécurité de l'information et cybersécurité

2.1 Risques inhérents à une société numérique

L'importance de certaines informations n'est souvent perçue qu'après la survenue d'un incident et des dommages qu'il cause. La perte, le vol, la divulgation non autorisée et l'utilisation abusive d'informations peuvent avoir de graves conséquences non seulement pour les autorités, mais aussi pour les entreprises et les particuliers. Les infrastructures d'information et de communication ainsi que les différents outils informatiques que les autorités et les entreprises emploient pour assister leurs processus d'affaires sont vulnérables. Une panne touchant l'exploitante d'une infrastructure critique indispensable au fonctionnement de la société, de l'économie, du canton ou de la Confédération peut entraîner des conséquences catastrophiques, voire la perte de vies humaines.

Une panne des outils TIC d'un hôpital, où sont enregistrés les données de la patientèle, des diagnostics et des traitements et où les machines d'assistance vitale sont connectées à Internet en fournit une illustration. Ce serait également le cas d'une défaillance du réseau de télécommunication de la centrale d'appels d'urgence de Berne. De la même manière, une panne du serveur de la Confédération exploitant le logiciel d'établissement du certificat COVID entraverait considérablement la liberté de déplacement et l'organisation des loisirs d'une très grande partie de la population. Dernier exemple : les transports publics et les fournisseurs d'énergie publics ou privés gérés à l'aide d'outils informatiques, dont le dysfonctionnement aurait de lourdes répercussions.

2.2 Objectifs stratégiques

Le canton de Berne avance résolument vers la cyberadministration et aspire à la primauté du numérique dans l'administration. Il définit ainsi sa vision en la matière au point 4 de la Stratégie pour l'administration numérique (SAN) du 26 juin 2019 :

> *La cyberadministration va de soi : des prestations de services des autorités à la fois transparentes et efficaces, fournies par voie électronique sans rupture de support à la population, aux acteurs économiques et à l'administration.*

Le Grand Conseil a inscrit la primauté de l'administration numérique à l'article 5 LAN :

> *[1] Les autorités agissent, informent et communiquent par voie électronique, à moins qu'elles ne puissent accomplir efficacement leurs tâches sous cette forme.*
> *[2] La forme de document déterminante au plan juridique est la forme numérique.*
> *(…)*

La protection des informations et des données personnelles est capitale pour la gouvernance étatique, en particulier pour la réputation des autorités, qui est un facteur crucial de la confiance placée en elles. C'est pourquoi la SAN subordonne sa mise en œuvre au principe suivant (point 6) :

> *Fiabilité et sécurité : La mise en œuvre de nouvelles solutions considère d'emblée le besoin législatif, la protection des données et la sûreté de l'information.*

Pour la même raison, la Stratégie sur la sécurité de l'information BE 2022 à 2025 du 14 décembre 2021 formule également ainsi la vision de la sécurité de l'information au sein de l'administration cantonale :

Les DIR/CHA/JUS garantissent dans tous les domaines une sécurité de l'information uniforme et optimale :

- *elles agissent en pleine conscience de la sécurité et de leur responsabilité dans un environnement numérique,*
- *elles prennent des mesures adéquates aux risques pour protéger leurs informations et leurs valeurs.*

Les DIR/CHA/JUS mettent à disposition les ressources nécessaires à la mise en œuvre des objectifs et des consignes concernant la sécurité de l'information.

L'administration cantonale met dès lors en œuvre les objectifs de sécurité et les orientations stratégiques ainsi définis – dont fait partie la LSIC.

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.

2.3 Signification et contenu

Ce ne sont pas tant les déficiences techniques des outils TIC que les faiblesses humaines, par exemple problèmes financiers ou tendance délictueuse, qui menacent la sécurité de l'information et la cybersécurité. En conséquence, le dispositif réglementaire de la LSIC doit comporter non seulement des mesures de sécurité techniques, mais aussi des mesures applicables aux collaboratrices et collaborateurs et au personnel d'encadrement.

Les informations et les données personnelles doivent être protégées en employant les techniques et pratiques de dernière génération, de sorte à garantir le fonctionnement infaillible de l'État (informations factuelles) d'une part et, d'autre part, à protéger aussi les droits fondamentaux et en particulier la sphère privée et intime (vie familiale, maladies, vie sexuelle) des personnes physiques (données personnelles).

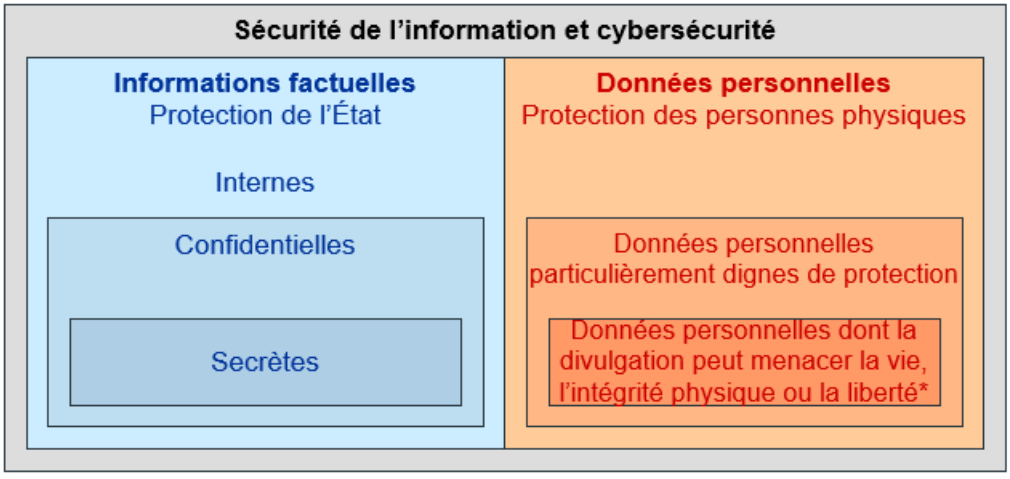

Illustration 1 : zone d'impact, objectifs et contenu de la sécurité de l'information et de la cybersécurité

*Exemples : informations sur des personnes du canton travaillant pour le Service de renseignement de la Confédération ou en qualité d'agents infiltrés dans le cadre de la lutte contre le crime organisé ou informations sur un parent craignant que ses enfants soient enlevés par l'autre. Selon la LCPD, les données personnelles ne forment pas une catégorie particulière, mais elles nécessitent une protection renforcée en raison du danger qu'elles peuvent représenter (art. 14, al. 1 LCPD).

La protection des données, qui est inscrite dans la Constitution et dans la loi, n'est garantie que si la sécurité de l'information et la cybersécurité sont assurées au moyen des techniques et pratiques de dernière génération et qu'elles préservent les aspects suivants :

a) Confidentialité
L'accès aux informations doit être réservé aux personnes habilitées. La divulgation illicite d'informations peut constituer une grave atteinte au secret de fonction, au secret professionnel et au secret commercial ou à la personnalité de particuliers, par exemple la communication des facteurs de comorbidité d'une personne ayant contracté le COVID ou de l'adresse exacte des centres de stockage des vaccins contre le COVID.

b) Intégrité
Les informations doivent être exactes, complètes et à jour, ce qui signifie qu'elles doivent autant que possible être infalsifiables, au risque de causer des dommages pouvant aller jusqu'à causer des décès, par exemple en cas d'erreur concernant les facteurs de comorbidité d'une personne atteinte du COVID ou le certificat de vaccination véritable et infalsifiable délivré aux personnes effectivement vaccinées contre le COVID.

c) Disponibilité
Les informations doivent être disponibles au moment où elles sont nécessaires, sous peine d'empêcher ou de fausser des décisions importantes. Exemples : les informations nécessaires à Swissmedic pour autoriser des vaccins contre le COVID ou l'application mobile « COVID certificate ».

d) Traçabilité
Les informations doivent pouvoir être répertoriées selon leur source, leur circuit et leurs dates de traitement. Il doit être possible d'établir qui a traité quelle information à quel moment. Exemple : le certificat COVID doit indiquer qui s'est fait vacciner, à quelle date et quelle autorité a délivré le certificat.

e) Cybersécurité
Elle est garantie lorsque les quatre critères de sécurité de l'information ci-dessus sont remplis lors du traitement ou de l'échange d'informations par l'intermédiaire d'infrastructures d'information et de communication - en particulier Internet (art. 3, lit. *a* de l'ordonnance fédérale sur les cyberrisques)[8]. Exemple : le serveur de la Confédération doit être accessible par Internet pour pouvoir vérifier la validité du certificat COVID.

Seul un dispositif de sécurité de l'information et de cybersécurité réellement performant permet de répondre aux objectifs de protection des données, à savoir la protection et l'exactitude des données personnelles, qui relèvent du droit fondamental de protection de la sphère privée garanti par la Constitution (art. 12, al. 3 et 18 de la Constitution cantonale réglant respectivement la protection de la sphère privée et celle des données[9], cf. graphique ci-dessus).

[8] OPCy, RS 120.73 ; https://www.fedlex.admin.ch/eli/cc/2020/416/fr#art_3
[9] ConstC, RSB 101.1 ; https://www.belex.sites.be.ch/app/fr/texts_of_law/101.1/versions/2420

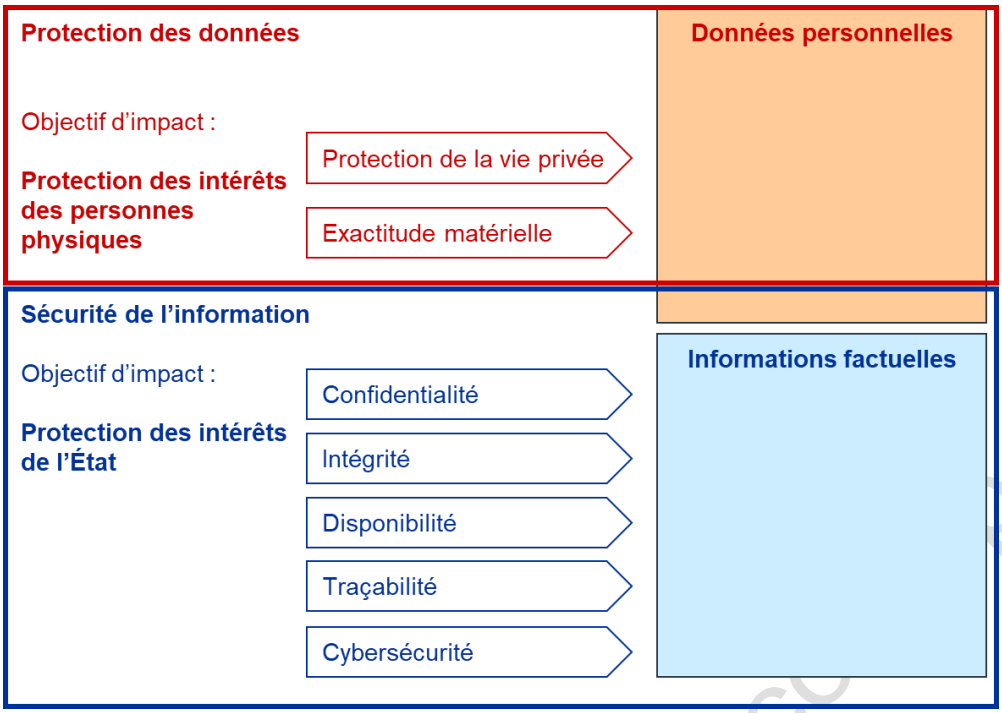

Illustration 2 : La sécurité de l'information et la cybersécurité, condition sine qua non à la protection des données

Les explications ci-dessus montrent que la sécurité de l'information et la cybersécurité posent non seulement des exigences spécifiquement techniques, mais aussi et surtout des exigences matière de droit, d'organisation, de processus et en particulier envers les personnes et leur hiérarchie. Elles concernent toutes les affaires de gestion publique, ce qui explique leur extrême complexité.

3. Rappel

3.1 Confédération

La LSI, que l'Assemblée fédérale a adoptée le 18 décembre 2020, entrera en vigueur le 1er avril 2023. Les cantons travaillent avec des informations et des données personnelles de la Confédération et utilisent ses applications, par exemple dans les domaines de la circulation routière, des poursuites pénales, des affaires militaires ou du Service de renseignement. C'est pourquoi la LSI exige des cantons soit qu'ils se dotent de dispositions équivalentes, soit qu'ils adoptent sa réglementation, spécialement conçue pour les vastes tâches de la Confédération (art. 3 LSI, Application de la loi aux cantons). Le présent projet de loi correspond à la première solution. Il adapte donc les dispositions fédérales à la situation bernoise, ce qui le rend à la fois plus efficace et plus économique.

3.2 Canton de Berne

3.2.1 Contexte

L'analyse de la législation bernoise relative à la sécurité de l'information et à la cybersécurité (Analyse des bases légales datant du 30 octobre 2019, réalisée dans le cadre du projet Sécurité de l'information BE) est parvenue aux conclusions suivantes :

1. Le canton de Berne ne dispose d'aucune règle de droit formelle, à caractère général et abstrait fixant les objectifs, le contenu, la structure et les processus relatifs à la sécurité de l'information et à la cybersécurité. Les autorités bernoises ne disposent donc d'aucune définition commune des notions de sécurité de l'information et de cybersécurité, ni, par voie de conséquence, de règles

uniformes pour les mettre en œuvre.

2. Les exigences actuelles en matière de sécurité de l'information et de cybersécurité concernent exclusivement les données personnelles et ne sont fixées qu'à l'échelon de l'ordonnance et encore, de manière incomplète, mal articulée et uniquement dans le contexte de la protection des données (ordonnance de 2008 sur la protection des données, OPD)[10]. Ni la cybersécurité, ni la protection des informations factuelles ne sont réglementées.

3. Un seul acte législatif règle la classification, à savoir l'ordonnance sur la classification, la publication et l'archivage des documents relatifs aux affaires du Conseil-exécutif (ordonnance sur la classification, OCACE)[11], mais il ne s'applique qu'à des documents (et non à des informations) de l'administration cantonale et vaut uniquement pour les affaires du Conseil-exécutif. Aucune disposition ne règlemente la classification et le traitement des autres informations, qu'elles soient imprimées, numériques ou orales. Toute la charpente de la sécurité de l'information et de la cybersécurité fait défaut dans le canton de Berne.

4. L'ordonnance de Direction de 2011 concernant la sûreté de l'information et la protection des données (OD SIPD)[12] ne règle pas non plus la protection des informations ou des objets, comme les hôpitaux et les établissements d'exécution des peines.

5. En guise d'organisation de la sécurité dans toute l'administration, l'OD SIPD se borne à désigner et assigner les responsables de la sécurité informatique (RSI) dans chaque DIR/CHA/JUS ainsi que la personne déléguée à la sécurité informatique, qui est responsable de la sécurité pour toute l'administration, de la même manière que la personne déléguée à la protection des données. Le canton de Berne ne dispose donc pas non plus d'une organisation de la sécurité efficace et limitant les coûts.

3.2.2 Objectif

3.2.2.1 Motion « Sécurité de la communication et échange des données »

La motion « Sécurité de la communication et échange des données » du 28 novembre 2018[13] traite de l'échange d'information et de données personnelles au sein de l'administration. Voici ce qu'a décidé le Grand Conseil le 10 novembre 2019 à l'issue de la délibération de cette motion :

Les Conseil-exécutif est chargé de faire en sorte et plus exactement de garantir

1. *qu'à tous les niveaux de l'administration et au sein de la police de Berne, ce soient toujours les logiciels et les applications les plus sûrs qui sont utilisés pour la communication électronique :*
   Adoption et classement.
2. *que dans les écoles aussi, des logiciels et des applications sûrs soient utilisés pour la communication :*
   Adoption sous forme de postulat.
3. *que les données soient enregistrées et conservées sur des serveurs suisses :*
   Adoption.
4. *qu'en ce qui concerne également la communication avec des externes, lorsqu'il s'agit de données et de documents dignes de protection, des logiciels et des applications sûrs soient utilisés pour la communication.*

[10] OPD, RSB 152.040.1 ; https://www.belex.sites.be.ch/app/fr/texts_of_law/152.040.1/versions/2001
[11] OCACE, RSB 152.17 ; https://www.belex.sites.be.ch/app/fr/texts_of_law/152.17/versions/1578
[12] OD SIPD, RSB 152.040.2 ; https://www.belex.sites.be.ch/app/fr/texts_of_law/152.040.2
[13] Motion 277-2018

3.2.2.2 Stratégie pour une administration numérique – plan stratégique 2021

Par arrêté du 20 janvier 2021, le Conseil-exécutif a lancé l'élaboration de la LSIC et le projet Sécurité de l'information BE (SI BE) avec l'objectif de « *faire fortement progresser la numérisation, de créer des bases décisives pour des projets de numérisation spécifiques et de contribuer de façon significative à la mise en œuvre de la stratégie [pour une administration numérique]* ».

La LSIC constitue la base légale et donc la condition nécessaire à la mise en place, dans le canton de Berne, d'un dispositif de sécurité de l'information et de cybersécurité uniforme, global, efficace et limitant les coûts.

4. Caractéristiques de la nouvelle réglementation

4.1 Architecture des normes

Dans le canton de Berne, les quatre lois ci-dessous sont soit déjà en vigueur soit en cours d'élaboration :

- Loi sur les fichiers centralisés de données personnelles (LFDP)[14], entrée en vigueur le 1er mars 2021.
- Loi sur l'administration numérique (LAN)[15], que le Grand Conseil a examinée en seconde lecture et adoptée lors de sa session de printemps de 2022.
- Loi sur la protection des données (LCPD), dont la Direction de l'intérieur et de la justice a lancé la révision à l'été 2020.
- Loi sur la sécurité de l'information et la cybersécurité (LSIC), proposée ici.

Ces lois forment les quatre piliers de la sécurité de l'information et de la protection des données :

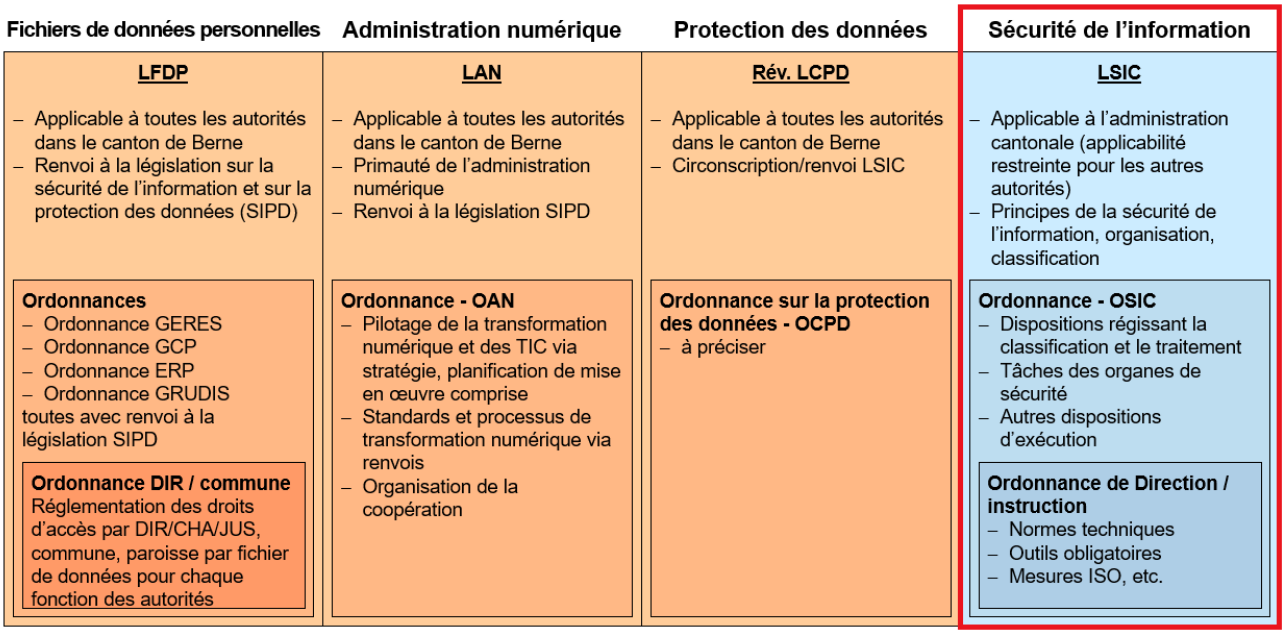

Illustration 3 : les quatre piliers de la législation bernoise en matière de sécurité de l'information et de protection des données

[14] RSB 152.05: https://www.belex.sites.be.ch/app/fr/texts_of_law/152.05
[15] ACE 750/2021 : LAN, proposition du Conseil-exécutif à l'intention du Grand Conseil du 16 juin 2021

4.2 Hiérarchie des normes

La LSIC donne un fondement au dispositif réglementaire de pilotage et de gestion de la sécurité de l'information et de la cybersécurité du canton de Berne. Ce dispositif prend appui sur les normes à caractère général et abstrait de la LSIC et de l'OSIC et s'étend jusqu'aux règles à caractère individuel et concret de réalisation d'un projet, de mise en œuvre de mesures de réduction du risque ou de désignation des personnes appelées à exercer une fonction critique dans l'administration bernoise :

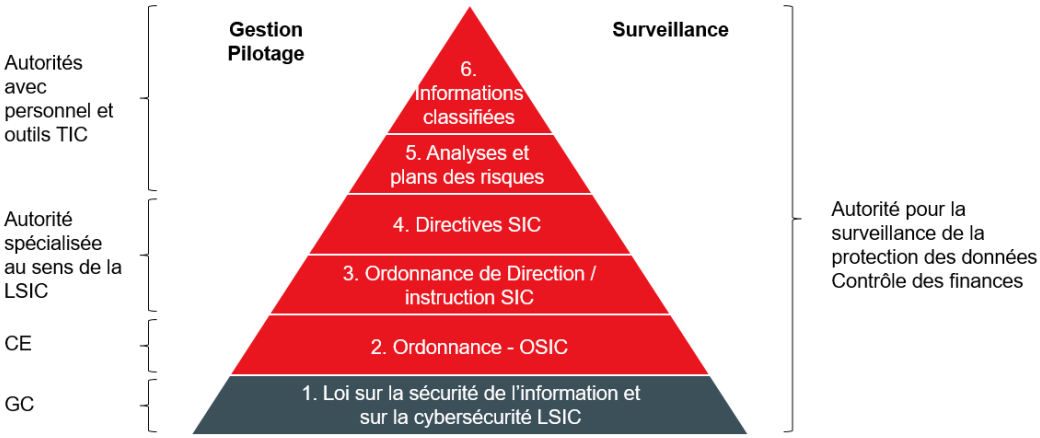

Illustration 4 : Fondements du pilotage et de la gestion de la sécurité de l'information et de la cybersécurité

4.3 Synthèse du contenu

La LSIC est bien plus courte et plus claire que la LSI de la Confédération, qui compte plus de 100 articles. D'abord parce qu'elle n'a pas besoin de réglementer les thèmes ne concernant que la Confédération avec ses besoins sécuritaires spécifiques (armée, Service de renseignement, politique étrangère, etc.) et, deuxièmement, du fait que les dispositions détaillées ne revêtant aucun caractère stratégique fondamental et ne portant pas atteinte aux droit fondamentaux sont reléguées à l'échelon de l'ordonnance ou des instructions, afin de pouvoir rapidement adapter les dispositions à l'évolution de la technique et des risques. Aucune règle portant sur la sécurité physique des infrastructures sensibles n'est inscrite dans la LSIC : d'une part, cela ne relève pas de la sécurité de l'information et, d'autre part, les mesures de protection fondées sur les risques qui ont déjà été prises ne nécessitent pas de base légale particulière (la vidéosurveillance est déjà réglée par la loi sur la police).

Il est notoire que l'être humain représente toujours la plus grande menace contre la protection de l'information. Des personnes endettées ou faibles de caractère peuvent être séduites par la corruption ou d'autres actes délictueux. C'est pourquoi de nombreux offices demandent d'ores et déjà un extrait de casier judiciaire et du registre des poursuites à certains membres de leur personnel. Ainsi l'Office de l'informatique et de l'organisation (OIO), l'Office du personnel (OP), l'Intendance des impôts (ICI) et l'Office de la circulation routière et de la navigation (OCRN) ont adopté cette pratique. Ces documents sont également réclamés à toutes les personnes qui se présentent à l'élection des juges, celle-ci relevant du Grand Conseil. À ce jour, seule la police dispose d'un fondement légal explicite à cet usage, et ce aux articles 160 et suivants de la loi sur la police (LPol)[16]. En matière de protection, les besoins de la police et de l'Office de l'exécution judiciaire (OEJ) dépassent en outre la seule sécurité informatique, compte tenu de leurs objets (installation de gestion des interventions et prison) et des entreprises qu'ils mandatent.

[16] RSB 551.1 ; https://www.belex.sites.be.ch/app/fr/texts_of_law/551.1/versions/2231

4.4 Objectifs d'effet

Outre la sécurité de l'information et la cybersécurité, qui constituent ses principaux objectifs, le dispositif réglementaire de la LSIC doit en outre produire les effets suivants :

a) Créer une compréhension commune des échelons de classification INTERNE, CONFIDENTIEL et SECRET.
b) Diminuer la quantité d'informations classifiées en uniformisant et en clarifiant les consignes légales en la matière :

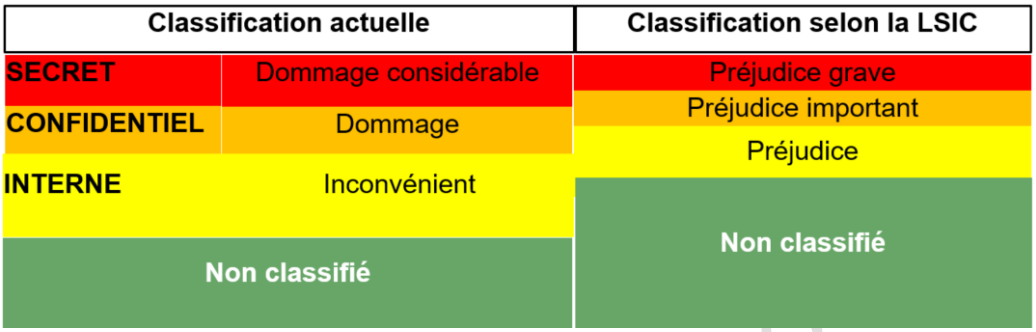

Illustration 6 : Diminution des classifications par la LSIC

c) Réduire le coût des mesures de sécurité en diminuant la quantité d'informations classifiées grâce à une classification ciblée, adaptée aux risques : « une place pour chaque chose et chaque chose à sa place ».
d) Définir, dans les actes législatifs d'exécution, des dispositions cohérentes de gestion des informations classifiées, valables pour l'ensemble des autorités et à tous les échelons de traitement.
e) Garantir que le personnel, et en particulier les cadres, prêtent l'attention nécessaire à la sécurité de l'information et à la cybersécurité (sensibilisation).
f) Fournir aux cadres des outils leur permettant d'identifier les faiblesses que leurs collaboratrices et collaborateurs représentent en matière de sécurité de l'information et de cybersécurité.
g) Organiser la sécurité en définissant clairement les responsabilités, les tâches et les compétences.

5. Forme de l'acte législatif

Compte tenu de leur caractère fondamental et stratégique d'une part et des graves atteintes aux droits des personnes qu'implique le contrôle de sécurité relatif aux personnes d'autre part, la sécurité de l'information et la cybersécurité doivent être encadrées par une loi. Les dispositions d'exécution seront définies par des ordonnances, des ordonnances de Direction ou des instructions (cf. point 4.2 ci-dessus).

6. Droit comparé

6.1 Confédération

Adoptée par le Parlement fédéral le 18 décembre 2020, la LSI entrera en vigueur le 1er avril 2023. Les cantons travaillent avec des informations et des données personnelles de la Confédération et utilisent ses applications, par exemple dans les domaines de la circulation routière, des poursuites pénales, des affaires militaires ou du Service de renseignement. C'est pourquoi la LSI exige des cantons soit qu'ils se dotent de dispositions équivalentes, soit qu'ils adoptent sa réglementation, spécialement conçue pour les vastes tâches de la Confédération (art. 3 LSI, Validité pour les cantons). Compte tenu de son volume et de son étendue, la LSI ne conviendrait pas pour le canton de Berne, raison pour laquelle est élaborée la LSIC (cf. point 4.3 plus haut).

6.2 Cantons

L'examen des législations des autres cantons au début de l'année 2022 a montré qu'il n'existe aucun modèle dont pourrait s'inspirer le canton de Berne. En effet, aucun canton ne s'est encore doté d'une loi similaire. Deux cantons, Zurich et Fribourg, ont réglementé la sécurité de l'information et la cybersécurité à l'échelon de l'ordonnance : Zurich applique le large dispositif réglementaire de la norme ISO 27001 à l'échelon de son administration ; compte de tenu de la LSI et étant donné qu'il a l'intention d'intégrer aussi les autres autorités, il étudie cependant l'opportunité de se doter d'une loi. Quant à Fribourg, son ordonnance ne réglemente que la sécurité des données personnelles.

7. Mise en œuvre, évaluation

Les projets de mise en œuvre et leur planning suivent le calendrier de mise en œuvre de la Stratégie SI BE (cf. illustration 6, p. 16 de cette stratégie) :

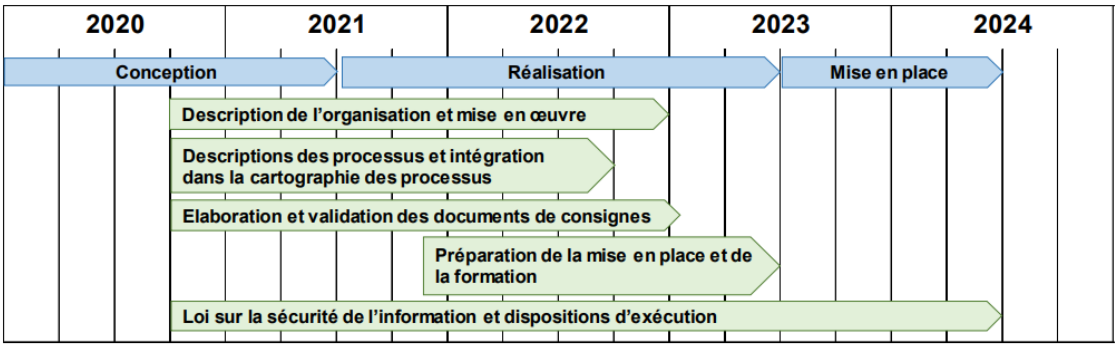

Illustration 7 : Mise en œuvre de la LSIC, projet SI BE compris

La mise en œuvre sera évaluée dans des processus d'amélioration continue à élaborer dans le cadre de la mise en œuvre.

8. Commentaire article par article

8.1 Dispositions générales

Article 1 – But

L'alinéa 1 énonce que la loi porte à la fois sur les informations en tant que telles et sur les outils utilisant les technologies de l'information et de la communication (outils TIC). La loi ne fait en principe aucune différence entre « informations » et « données », la notion d'information recouvrant les deux. Elle définit le terme « outils TIC » à l'article 4, lettre *d*.

Alinéa 2 : la sécurité n'est pas une fin en soi. Son rôle est de protéger les intérêts publics cités. La loi protège donc en premier lieu les intérêts des autorités du canton de Berne, ce qui agit toutefois directement sur la confiance que les tiers placent en elles. La LSIC protège donc les intérêts publics suivants :

a) L'objectif central de cette loi est de préserver la capacité de décision et d'action des autorités (lit. *a*). Pour accomplir les missions que leur confèrent la Constitution et la loi, les autorités doivent pouvoir compter sur la disponibilité, l'intégrité et la traçabilité de leurs informations et, dans certains cas, sur la fiabilité de l'infrastructure informatique.

b) La lettre *b* vise en premier lieu les informations des domaines de la police, du renseignement (sur mandat de la Confédération) et de certains secteurs de l'approvisionnement du pays (réserves obligatoires cantonales) ainsi que les moyens mis en place par les autorités pour assurer la sécurité. Ces informations sont souvent hautement confidentielles, car leur utilisation abusive peut avoir des conséquences vitales pour l'État, la population ou certaines personnes ou groupes de personnes. Pour la même raison, les autorités doivent pouvoir compter sur la disponibilité et le fonctionnement permanents des outils TIC qu'elles emploient pour les assister dans des tâches de sécurité critiques, et ce, même en temps de crise.

c) La lettre *c* porte sur les obligations légales et contractuelles que les autorités doivent respecter pour protéger les informations qui ne tombent pas sous le coup des lettres *a* et *b*. Elle met en œuvre la conformité légale et contractuelle de la protection de l'information.

   Pour accomplir leurs tâches légales, les autorités traitent une très grande quantité d'informations, qu'elles doivent protéger en vertu des dispositions légales les plus diverses (loi sur la protection des données, loi sur les impôts, loi sur la police, loi sur les avocats et les avocates, etc.) ou qu'elles reçoivent de tiers à l'unique condition d'en garantir une protection adéquate.

   Les secrets professionnel ou commercial, le secret de fabrication ou la préservation du caractère confidentiel et de l'intégrité de données personnelles ne servent certes pas directement les intérêts des autorités elles-mêmes. Celles-ci sont néanmoins tenues de protéger ces informations, que ce soit en vertu d'une loi ou d'un contrat. Qu'elles manquent notoirement à cette obligation et leur crédibilité en pâtit, ce qui entrave considérablement leur capacité d'action. Sans compter que leurs organes sont alors passibles de poursuites au pénal et au civil.

   La lettre *c* embrasse donc toutes les informations que les autorités doivent traiter et protéger, mais qui ne sont pas nécessairement classifiées. Elle protège également l'intérêt des autorités à la préservation de leur crédibilité.

Article 2 – Champ d'application

En ce qui concernant son champ d'application, la LSIC reprend l'approche de la LSI. Selon cette dernière, ne s'appliquent aux cantons que les dispositions relatives aux informations classifiées, lorsque les cantons traitent des informations classifiées de la Confédération, et à la sécurité des moyens informatiques, lorsque les cantons accèdent à des moyens informatiques de la Confédération (art. 3, al. 1 LSI). La loi précise que ces dispositions ne s'appliquent pas aux cantons s'ils garantissent une sécurité de l'information au moins équivalente (art. 3, al. 2 LSI). Cette dernière condition sera remplie avec l'entrée en vigueur de la LSIC.

Sur le même modèle, la LSIC, dans son ensemble, vaut exclusivement pour les autorités cantonales. 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).

Article 3 – Relation avec d'autres lois

Une classification ne restreint pas automatiquement le principe de publicité réglé aux articles 27 et suivants de la loi sur l'information et l'aide aux médias (LIAM ; RSB 107.1). Selon le cas, elle peut

néanmoins constituer un indice de la présence d'un intérêt public ou privé prépondérant susceptible d'interdire l'accès aux documents officiels (al. 1).

Certains actes législatifs particuliers, comme les lois sur la protection des données, sur le Grand Conseil, sur les impôts, sur la santé publique ou sur les avocats et les avocates, règlent l'obligation de garder le secret pour leur champ d'application. Ces dispositions l'emportent si elles divergent de la LSIC (al. 2). À cet égard, la distinction entre la notion d'information selon la LSIC et celle de données personnelles selon la LCPD est particulièrement importante. La LCPD régit la protection de la personnalité et des droits fondamentaux des personnes que les autorités cantonales doivent garantir lorsqu'elles traitent des données personnelles (art. 1, But). Elle dispose notamment que les autorités doivent traiter les données personnelles conformément à la loi, dans le respect du principe de proportionnalité, dans un but déterminé et de la manière la plus transparente possible pour les personnes concernées (art. 5, Admissibilité du traitement de données personnelles). Elle précise que le traitement des données personnelles obéit aux règles qu'elle édicte.

Toutefois, la LSIC complète la LCPD pour ce qui concerne les exigences relatives à la disponibilité, à l'intégrité des données personnelles et à la *protection effective* de la confidentialité. Par exemple, l'article 17 LCPD exige concrètement que toute personne qui traite des données personnelles veille à leur sécurité. De leur côté, les articles 4 à 6 OPD concrétisent les exigences de protection des données personnelles en spécifiant notamment que les mesures techniques et organisationnelles doivent intégrer les dernières évolutions techniques, sans pour autant définir ce qu'est l'évolution technique ni qui a la responsabilité de la définir. À terme, c'est la LSIC et ses dispositions d'exécution, en particulier l'ordonnance, qui s'appliqueront sur ces points. La confidentialité, la disponibilité, l'intégrité et la traçabilité doivent aussi être garanties en matière de données personnelles. Or celles-ci sont rarement classifiées explicitement, car la classification est réservée à la protection des intérêts publics du canton au sens strict selon l'article 1, alinéa 2 LSIC. Les données personnelles ne sont classifiées qu'à titre exceptionnel, lorsqu'il est nécessaire de protéger à la fois la personne physique en vertu de la LCPD et l'intérêt public en vertu de la LSIC. C'est le cas notamment des données personnelles particulièrement dignes de protection des conseillères et conseillers fédéraux.

Par conséquent, les dispositions d'exécution de la LSIC attribueront aux informations et aux données personnelles un niveau de protection dépendant non seulement des besoins mais aussi des critères de confidentialité, de disponibilité, d'intégrité et de traçabilité (voir à ce sujet l'illustration 8 dans le commentaire de l'art. 8). De cette manière, la standardisation des mesures en fonction des connaissances scientifiques et techniques les plus récentes, qui sera corrélée aux différents niveaux de protection, permettra aussi de satisfaire aux exigences de sécurité des données définies par la législation sur la protection des données et, du même coup, de renforcer la protection des données dans le canton.

Article 4 – Définitions

La LSIC protège les informations concernant les intérêts publics dignes de protection définis à l'article 1, alinéa 2 (lit. *a*).

Tel que le définit la lettre *d*, le terme *outils TIC* est un générique désignant tous les équipements utilisant les techniques de l'information et de la communication ; il est équivalent aux ressources TIC définies à l'article 4, alinéa 3, lettre *a* LAN. Des termes plus précis (système d'information, réseau, application, transmission de la voix humaine, téléphonie, etc.) seront utilisés et définis à l'échelon de l'ordonnance et des instructions. Un outil TIC peut aussi se composer de plusieurs systèmes ou outils formant une seule entité fonctionnelle.

8.2 Principes

Article 5 – Obligations des autorités en matière de sécurité de l'information et de cybersécurité

L'alinéa 1, lettre a oblige expressément les autorités à évaluer le besoin de protection des informations qui relèvent de leur domaine de responsabilité. Cela suppose déjà qu'elles sachent de quelles informations elles disposent. Elles doivent donc tenir un inventaire complet et à jour de leurs informations et données, qui est aujourd'hui identique à celui de tous les outils TIC contenant des informations ou des données. Les autorités doivent d'abord déterminer le besoin de protection à la lumière des intérêts publics à préserver, avant de pouvoir arrêter des mesures de protection adaptées aux risques qui soient à la fois efficaces et économiques, - selon le principe « une place pour chaque chose et chaque chose à sa place ». Un inventaire complet réalisé dans cet esprit ainsi qu'une analyse juste du besoin de protection préservent les intérêts publics, tout en permettant aux autorités d'économiser l'argent public. Car il ne serait évidemment pas rentable de classifier SECRET des informations qui ne présentent pas de danger particulier.

La lettre b énumère les quatre critères de protection garantissant la sécurité des informations, à savoir la confidentialité, l'intégrité, la disponibilité et la traçabilité, qui sont définis au point 2.3 plus haut.

La lettre c énonce explicitement le principe selon lequel les outils TIC doivent être convenablement protégés contre toute utilisation abusive, défaut et dérangement, même si cela découle déjà de la lettre *b*. Cette insistance se justifie par le fait que l'informatisation des processus d'affaires ne cesse de gagner du terrain. De nos jours, le bon fonctionnement des outils TIC est une condition indispensable à l'efficacité du travail des autorités.

La gestion des risques (*al. 2*) est la méthode centrale de la sécurité de l'information. Elle consiste à identifier et évaluer en permanence les risques menaçant la sécurité de l'information, à les prévenir ou à les réduire à un niveau tolérable, et à documenter les risques tolérables et leur acceptation. Cette démarche s'inscrit dans la gestion globale des risques mise en place par l'autorité.

L'évaluation des risques suppose
- une bonne connaissance des tâches légales et des processus d'affaires correspondants,
- une évaluation régulière des menaces,
- une analyse des points faibles,
- une estimation des probabilités d'occurrence et de l'étendue des dommages potentiels.

Les risques peuvent être évités - en renonçant purement et simplement à une activité trop risquée -, réduits - grâce à des mesures techniques, organisationnelles ou légales -, ou bien tolérés. Les risques tolérés doivent être clairement signalés et acceptés par les personnes décisionnaires.

L'alinéa 3 part du postulat que la sécurité absolue est un idéal inatteignable. La suppression de failles de sécurité minimes subsistantes peut nécessiter un travail disproportionné. Les autorités compétentes doivent donc veiller à ce que leurs mesures soient adaptées aux risques encourus et à la fois efficaces et économiques. En conséquence, les instances supérieures doivent soupeser les coûts et les avantages pour déterminer les mesures de sécurité à prendre. Si certaines entravent trop le travail, il est fort probable que le personnel ne les respectera pas, voire les contournera intentionnellement.

Article 6 – Tiers mandatés

Pour exercer leurs fonctions, les autorités sont souvent tributaires de prestations du secteur privé ou d'autres services. L'autorité qui doit mandater des tiers est tenue de veiller à ce que le mandat soit attribué et exécuté dans le respect des mesures de sécurité légales. Celles-ci sont en règle générale

stipulées dans le contrat. En principe, les mandataires ne doivent obtenir l'accès à des informations ou à des outils TIC des autorités que lorsqu'ils ont eux-mêmes mis en œuvre les mesures nécessaires. La LSIC commande également aux autorités de vérifier cette mise en œuvre de manière appropriée (c.-à-d. en fonction des risques). Elles peuvent procéder à ce contrôle en se rendant sur place ou en demandant au tiers de lui remettre un certificat écrit. Si le mandat confié comporte une activité sensible au plan de la sécurité, les autorités peuvent procéder aux contrôles de sécurité relatifs aux personnes (CSP) qui s'avèrent nécessaires (art. 17, al. 1, lit. *c*).

Article 7 – Réactivité et planification préventive

Il y aura toujours des incidents de sécurité. Il est donc nécessaire définir une approche uniforme et efficace à appliquer dans ces cas-là.

Selon l'alinéa 1, les autorités doivent prendre les mesures nécessaires (p. ex. des contrôles réguliers, des capteurs, des alarmes, une surveillance du réseau, des analyses périodiques des fichiers journaux) pour identifier précocement tout incident de sécurité. Elles doivent en outre définir la procédure à appliquer si un incident ou des failles de sécurité sont identifiés et attribuer des compétences claires pour la gestion de ces incidents. De plus, le personnel cantonal et les personnes extérieures au canton doivent connaître la conduite à tenir en la circonstance, afin d'en réduire les répercussions au minimum. Enfin, pour pouvoir tirer les leçons des incidents survenus, elles doivent en déterminer les causes et les analyser.

De surcroît, les autorités et surtout leur exécutif doivent prendre toutes les dispositions nécessaires pour pouvoir accomplir leurs missions essentielles dans les délais, y compris dans des situations exceptionnelles (démarche que l'on appelle la gestion de la continuité des activités [BCM, de l'anglais Business Continuity Management]). De nos jours, l'accomplissement de toutes les tâches des autorités ayant une grande importance pour la population est tributaire de la fiabilité des outils TIC utilisés. C'est pourquoi l'alinéa 2 dispose que les autorités doivent identifier celles de leurs tâches qui sont stratégiquement indispensables, se doter de plans d'action en cas d'atteinte grave à la sécurité de l'information et à la cybersécurité (p. ex. panne durable d'un système) et organiser des exercices pour s'entraîner à les appliquer si cela est adapté aux risques. Étant donné que les risques et les atteintes à la sécurité de l'information qu'ils sont susceptibles d'entraîner peuvent constamment évoluer, il faut périodiquement réviser et actualiser les plans d'action.

8.3 Mesures concernant l'organisation

Article 8 – Classification

En classifiant les informations, les autorités déterminent à quel point il est important que ces informations ne tombent pas dans les mains de personnes non autorisées. Les mesures correspondantes sont définies par voie d'ordonnance.

Alinéa 1 : le critère déterminant la classification est l'intérêt public à la protection d'informations, à l'exception de l'intérêt public défini à l'article 1, alinéa 2, lettre *c*, qui ne constitue pas un motif de classification en soi (cf. les remarques à ce sujet). En conséquence, les données personnelles selon la LCPD et les secrets commercial, professionnel ou de fabrication ne sont pas classifiés, sauf si la classification de certaines informations est nécessaire pour protéger les intérêts publics définis à l'article 1, alinéa 2, lettres *a* et *b*. Il en va de même des informations qui sont traitées par les tribunaux et le Ministère public dans le cadre de leurs procédures ordinaires. La plupart d'entre elles sont des données personnelles certes dignes de protection, mais dont la classification n'est pas nécessaire selon la présente loi. En revanche, les mesures particulières nécessaires pour protéger ces informations sont classifiées (p. ex. un plan de sécurité de l'information et de protection des données, plan SIPD).

Le plan ci-dessous repose sur cette distinction.

Loi sur la sécurité de l'information et la cybersécurité LSIC		**Ordonnance sur la sécurité de l'information et la cybersécurité OSIC**	**Loi sur la protection des données LCPD**
Protection des intérêts de l'État		*Exécution et mesures pour la sécurité de l'information et la cybersécurité (par analogie aussi pour la LCPD)*	*Protection des intérêts des personnes physiques*
Outils TIC	**Informations**	**Mesures de protection à la pointe de la technique**	**Données personnelles**
Protection très élevée	SECRET	Niveau de protection 3	Données personnelles représentant une grave menace pour la sécurité de l'intéressé·e (intégrité physique, vie, liberté)
Protection élevée	CONFIDENTIEL	Niveau de protection 2	Données personnelles particulièrement dignes de protection ou sous le sceau du secret (secret professionnel, fiscal, etc.)
Protection de base	INTERNE	Niveau de protection 1	Données personnelles générales
	Non classifié	Niveau de protection 0	Données non personnelles (hors du champ de protection de la LCPD)
CSP selon LSIC par service central spécialisé ou par autorité décentralisée.		Dispositions d'exécution de la LSIC et de la LCPD par l'intermédiaire de renvois	Contrôle de la probité des personnes selon la *loi sur le personnel* par autorité décentralisée

Illustration 8 : Plan de protection de la confidentialité ; frontière LSIC–LCPD ; OSIC en « interface »

Il est important de bien distinguer les objectifs de protection de la LSIC de ceux de la LCPD.

Le rôle primordial de la LSIC est de préserver l'État de toute entrave illicite à son action. La LCPD, quant à elle, a pour but de protéger les personnes contre les atteintes illicites à leur personnalité. La législation spécifique à la protection de ces deux intérêts (LSIC et LCPD) définit en conséquence leurs niveaux de protection respectifs. Ceux-ci seront synchronisés via les quatre niveaux de protection dans l'ordonnance sur la sécurité de l'information et la cybersécurité (OSIC) à élaborer. Si les objectifs de protection sont différents, les mesures sont les mêmes. Ainsi, seules les personnes qui travaillent régulièrement avec des informations classifiées CONFIDENTIEL ou SECRET doivent faire l'objet d'un contrôle de sécurité relatif aux personnes (CSP). Pour vérifier la probité de certaines personnes, les autorités d'engagement décentralisées traitant des données personnelles particulièrement dignes de protection peuvent toutefois elles-mêmes procéder à ces contrôles pour appliquer la loi sur le personnel (LPers[17] ; point 8.6 ci-dessous).

Alinéa 2 : l'échelon de classification se détermine en fonction de la gravité et de l'étendue du dommage qui pourrait être causé à l'intérêt public à protéger si l'information parvenait à la connaissance d'un tiers non autorisé. Quoique déterminants, ces deux critères de classification ne sont toutefois pas suffisants. Il doit également y avoir un lien de cause à effet clair entre le fait qu'un tiers non autorisé ait connaissance de l'information et le potentiel préjudice porté aux intérêts protégés. Il est donc nécessaire de tenir compte aussi de la fréquence, plus précisément de la probabilité de réalisation du dommage.

[17] LPers, RSB 153.01 : https://www.belex.sites.be.ch/frontend/versions/2253

Le graphique suivant illustre l'évaluation du risque :

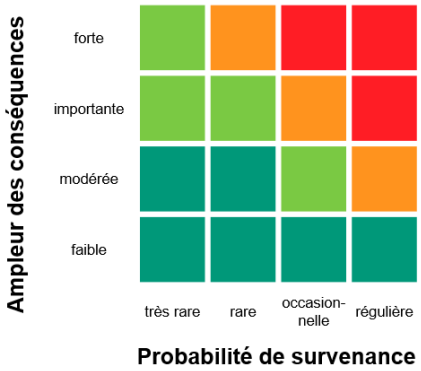

Illustration 9 : Matrice des risques selon norme BSI 200-3

La classification d'une information correspond donc au résultat d'une évaluation des risques et doit ainsi refléter le besoin de protection effectif de cette information.

Une retenue particulière est de mise lorsqu'il s'agit d'évaluer le besoin de protection d'informations de nature politique. L'article 1, alinéa 2, lettre *a* (capacité d'action) protège certes la libre formation de l'opinion et de la volonté des autorités. Mais dans une démocratie moderne, l'activité gouvernementale ordinaire suppose que les idées, propositions, plans et décisions fassent l'objet d'un débat public et de critiques pouvant le cas échéant être véhémentes. La classification ne doit donc pas revenir à soustraire des éléments au débat public alors qu'aucun intérêt public prépondérant ne le nécessite.

Lettre a : la décision de classifier repose sur la présence d'éléments fondés justifiant au moins la classification « INTERNE ». Le dommage potentiel ne doit donc pas être négligeable, mais au contraire perceptible. Dans le cas d'informations tombant sous le coup de l'article 1, alinéa 2, lettre *a*, le seuil de classification « INTERNE » peut être atteint relativement rapidement. Cette classification concerne d'ailleurs la plupart du temps ce type d'information. Ainsi, les documents de sécurité concernant les outils TIC ou les plans d'intervention des forces de sécurité sont en règle générale classifiés « INTERNE ».

Lettre b : la classification « CONFIDENTIEL » correspond à un besoin de protection supérieur à celui de la classification « INTERNE ». Le dommage potentiel doit être plus net et plus important, par exemple :

- entrave illégitime et temporaire à la libre formation de l'opinion et de la volonté des autorités,
- obstacle temporaire à la capacité d'action des autorités,
- entrave significative et de longue durée à l'accomplissement des tâches d'une autorité,
- impossibilité temporaire d'intervention de certaines forces de police ou de police sanitaire,
- menace pesant sur la sécurité de personnes ou de groupes de personnes,
- sabotage de fonctions sensibles de la régulation des crues à Thoune,
- dommage financier important causé au canton.

Lettre c : la formulation choisie pour la classification « SECRET » implique un dommage particulièrement important, de nature catastrophique pour les autorités, par exemple :

- obstacle temporaire ou entrave particulièrement sérieuse de plus longue durée à la capacité de décision et d'action d'une autorité,
- obstacle temporaire ou entrave sérieuse de plus longue durée à l'accomplissement de tâches indispensables par une autorité,
- impossibilité d'intervention d'importantes forces de police ou de police sanitaire,
- menace pesant sur la vie et l'intégrité physique de groupes de population entiers,

- panne d'équipements critiques fournissant des services indispensables,
- grave dommage financier causé à une commune ou au canton.

La mention de la classification doit être immédiatement visible et ne doit pas pouvoir être confondue avec d'autres indications. Sa mention en lettres capitales s'est imposée dans les relations internationales.

Alinéa 3 : la classification est obligatoire dès que les critères en sont réunis. Compte tenu du principe de publicité et des charges administratives inhérentes à la classification, celle-ci doit toutefois rester l'exception. Au bout d'un certain temps ou après une échéance précise (p. ex. publication d'un rapport ou terme d'une mesure concrète), des informations jusque-là classifiées ont souvent moins voire plus du tout besoin d'être protégées, par exemple parce qu'elles ne sont plus actuelles. Leur classification ne se justifie donc plus et n'aurait d'autre effet que de créer inutilement du travail. En outre, les informations qui doivent rester classifiées longtemps nécessitent d'autres dispositifs techniques de protection que celles dont la durée de protection est limitée. Dans les cas où il est impossible de fixer d'emblée un terme à la classification, il faut bien s'assurer que celle-ci est véritablement nécessaire. Le besoin de protection doit au moins être examiné dans le cadre de l'obligation de présenter les documents aux Archives de l'État prévue à l'article 9 de la loi sur l'archivage (LArch)[18].

Alinéa 4 : dans l'administration cantonale, la classification incombe actuellement à la personne qui crée un document, celle-ci étant la mieux placée pour déterminer le besoin de protection et évaluer les risques éventuels. Toutefois, les autorités peuvent aussi décider de confier cette compétence à leur direction, à un service central ou exclusivement à la hiérarchie par exemple. Le Conseil-exécutif réglementera ce point plus précisément par voie d'ordonnance, y compris la déclassification d'informations par les instances supérieures ainsi que d'archives.

Article 9 – Accès aux informations classifiées

L'alinéa 1 définit les conditions d'accès à des informations classifiées, l'accès étant lui-même le préalable au traitement de ces informations. Le principe consistant à donner l'accès exclusivement si nécessaire vaut pour toute information classifiée. Il n'existe donc aucun droit général à accéder à toutes les informations classifiées. La réglementation de l'accès à des informations classifiées régit aussi l'accès aux systèmes dans lesquels figurent ces informations.

Lorsque le droit d'accès est donné par contrat, ledit contrat doit autoriser l'accès à des informations classifiées et en régler le traitement. L'expression « offrir la garantie » d'une gestion conforme implique que les personnes appelées à traiter des informations classifiées aient été formées sur le sujet. Elles peuvent en outre avoir l'obligation d'apporter la preuve qu'elles ont la faculté de respecter les mesures de sécurité techniques et physiques nécessaires. Le traitement d'informations classifiées « CONFIDENTIEL » ou « SECRET » peut, en plus, être subordonné à un contrôle relatif aux personnes.

Article 10 – Accès en procédure spéciale

Alinéa 1 : les règles de procédure du Grand Conseil, concernant la publicité de ses organes et l'information du public selon les articles 11 et suivants de la loi sur le Grand Conseil (LGC)[19] par exemple, ainsi que celles des tribunaux et du Ministère public sont réservées. Elles s'appliquent donc à l'accès à des informations classifiées (p. ex. dans le cadre de leur utilisation comme base décisionnelle ou comme preuve). Les lois cantonales de procédure contiennent elles-mêmes des règles indiquant dans quelle mesure l'accès à ce genre d'information peut être donné aux parties à la procédure et dans quelle mesure elles peuvent être divulguées dans le cadre de procédures publiques ou dans

[18] LArch, RSB 108.1 : https://www.belex.sites.be.ch/app/fr/texts_of_law/108.1
[19] RSB 151.21 : https://www.belex.sites.be.ch/app/fr/texts_of_law/151.21/versions/1628

quelle mesure le droit de déposer peut être refusé aux témoins en vertu de leur obligation légale de garder le secret.

Alinéa 2 : avant d'autoriser la divulgation d'informations classifiées à des tiers, le service de classification doit néanmoins être entendu sur les motifs de la classification et sur les répercussions potentielles de la divulgation de ces informations. L'organe ou le tribunal compétent décide de la suite à donner en tenant compte de la position exprimée par le service de classification. Par exemple, si une commission parlementaire de surveillance veut citer un document classifié dans un rapport public ou si un tribunal veut faire de même dans un jugement public, ils doivent préalablement demander son avis au service de classification.

8.4 Mesures techniques

Article 11 – Procédure de sécurité

Les temps sont loin où les offices ou les tribunaux, par exemple, exploitaient eux-mêmes leurs propres outils TIC dans leurs locaux. Aujourd'hui, les autorités cantonales achètent en général leurs prestations informatiques auprès d'entreprises externes hautement spécialisées, principalement auprès de Bedag Informatique SA, qui appartient au canton, mais aussi auprès de sociétés privées. En conséquence, l'utilisation des outils TIC et leur exploitation ne relèvent pas de la même organisation, ce qui a d'importantes répercussions en matière de sécurité.

D'autant que la sécurité de l'information et la cybersécurité sont la plupart du temps considérées, à tort, comme une affaire purement technique dont sont responsables les mandataires. 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 en matière de sécurité de l'information et de cybersécurité). Le Conseil-exécutif doit les définir plus précisément dans une procédure de sécurité standardisée valable pour l'ensemble des autorités. En vertu de l'ordonnance de Direction de 2011 concernant la sûreté de l'information et la protection des données (OD SIPD), toutes les autorités cantonales ont d'ores et déjà l'obligation d'appliquer une procédure de ce genre. Ces dispositions doivent toutefois être systématisées et adaptées à la technique et aux risques actuels. 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. Cette procédure de sécurité doit en particulier définir les tâches, compétences et responsabilités en matière de sécurité des services qui planifient l'utilisation d'outils TIC et en décident.

Étant donné que cette procédure doit être régulièrement adaptée aux nouvelles techniques et aux nouveaux risques, le Conseil-exécutif peut déléguer sa définition à un organe spécialisé compétent pour tout le canton, a priori la Conférence pour l'administration numérique et les TIC (CNT ; cf. point 11 ci-dessous).

L'alinéa 2 énumère les principaux éléments clés de cette procédure :

Lettre a : besoin de protection

Les outils TIC sont utilisés dans des buts précis et pour une certaine durée de vie, planifiée à l'avance. Pour définir le but de leur utilisation, la première étape consiste à déterminer les processus d'affaire qu'ils doivent assister ainsi que les informations qu'ils doivent servir à traiter. À ce stade, c'est-à-dire durant la phase de planification, l'autorité doit évaluer le besoin de protection de ces informations selon l'article 5, alinéa 1 ainsi que les répercussions qu'une panne ou une utilisation abusive de ces outils pourraient avoir sur les intérêts publics définis à l'article 1, alinéa 2. Ce bilan d'impact sur l'activité doit être réalisé par le service responsable du processus d'affaire. Pour évaluer le besoin

de protection, il faut aussi tenir compte du fait que l'outil TIC s'insère dans un environnement technique et professionnel (que l'on appelle une architecture). Un repérage des interconnexions et interdépendances effectué en amont contribue également à concrétiser les mesures là où elles sont le plus efficaces. L'analyse du besoin de protection permet de classer les outils TIC à l'un des échelons de sécurité prévus à la lettre *b* (ci-après) et de définir les exigences auxquels ils doivent répondre en matière de protection des informations pour être conformes à l'article 12.

Lettre b / alinéa 3 : échelon et mesures de sécurité

Les outils TIC sont classés à un échelon de sécurité en fonction des dommages que causerait une atteinte à la sécurité des informations qu'ils servent à traiter. Ces échelons sont ceux prévus à l'article 17 LSI.

- L'échelon « protection de base » vaut pour tous les outils TIC qui ne présentent aucun besoin particulier de protection ; il permet le traitement d'informations non classifiées ou classifiées INTERNE.
- L'échelon « protection élevée » est prévu pour les outils TIC pouvant être à l'origine de dommages importants ; il permet de traiter des informations classifiées CONFIDENTIEL au plus.
- L'échelon « protection très élevée » vaut pour les outils TIC pouvant être à l'origine de dommages très importants ; il permet le traitement d'informations de n'importe quelle classification, y compris SECRET.

Des mesures de sécurité standardisées et adaptées au risque sont définies pour chaque échelon, par exemple la procédure de connexion, le cryptage et la conduite à tenir avec les supports de données et les appareils.

Lettre c : mise en œuvre et contrôle des mesures de sécurité

Les autorités doivent déterminer les mesures à prendre et la manière de contrôler leur mise en œuvre. En principe, il faut appliquer des mesures standardisées correspondant au niveau de protection défini par l'OSIC (cf. illustration 8 ci-dessus). Dans ce contexte, il est particulièrement important de contrôler la mise en œuvre de ces mesures.

Lettre d : attestation de sécurité

L'attestation de sécurité a pour but de garantir, avant toute utilisation d'un outil TIC, que l'autorité responsable connaît les risques identifiés qui subsistent et qu'elle est disposée à les assumer. Si elle pense qu'ils sont encore trop élevés, elle peut refuser l'attestation et réclamer des mesures supplémentaires de réduction des risques.

Lettre e : contrôle des risques

La sécurité de l'information et la cybersécurité ne sont jamais définitivement acquises. Les autorités doivent donc définir la marche à suivre pour adapter les outils TIC utilisés à l'évolution des risques.

Aux termes de *l'alinéa 4*, l'exécution de la procédure de sécurité incombe à l'autorité qui décide de l'utilisation d'outils TIC et mandate des tiers, au moyen de contrats-cadres par exemple. Il s'agit de l'autorité responsable de l'outil TIC selon le « modèle à trois couches » prévu à l'article 32, alinéa 2 LAN : l'Office d'informatique et d'organisation (OIO) pour les services TIC de base du canton et la Direction compétente ou l'office compétent pour les applications spécialisées et les applications de groupe.

Cette autorité répond seule de ses processus d'affaire et de la mise en œuvre des exigences de sécurité. Elle doit donc communiquer ses exigences métier et la sécurité à son mandataire de manière

claire et compréhensible sous une forme contraignante. Les autorités qui se procurent des outils TIC en passant des contrats-cadres peuvent se fier au résultat de la procédure de sécurité.

L'*alinéa 5* pose le principe de l'uniformisation, par voie d'ordonnance, des échelons de protection et des mesures correspondantes pour tous les outils TIC, informations et données personnelles présentant un besoin de protection comparable, conformément à l'option de mise en œuvre de l'illustration 8 plus haut.

Article 12 – Sécurité de l'exploitation

Cet article dispose clairement que l'autorité continue de répondre de l'exploitation sécurisée d'outils TIC même lorsqu'elle la confie à l'autorité compétente (art. 32, al. 2 LAN, cf. plus haut). Les diverses autorités chargées de l'exploitation d'un seul et même outil TIC peuvent régler différemment leur responsabilité respective dans des dispositions d'exécution ou des instructions (cf. art. 29, al. 2 LAN). En matière d'utilisation des services TIC de base par exemple, l'OIO répond de la sécurisation des postes de travail, des serveurs, des imprimantes, etc. de l'administration, tandis que les autorités qui s'en servent répondent de leur utilisation sécurisée par les membres de leur personnel.

La sécurité lors de l'utilisation d'outils TIC relève de la responsabilité principale du donneur d'ordre, autrement dit des autorités. De leur côté, les mandataires sont chargés d'exploiter ces outils TIC selon les connaissances les plus récentes et la technique de dernière génération. Ils ont l'obligation d'intégrer et d'appliquer les exigences et les mesures prévues dans la présente loi ainsi que les besoins supplémentaires définis contractuellement par les autorités.

Tout mandataire interne à l'autorité est une autorité tombant sous le coup de la présente loi et doit donc l'appliquer dans l'exercice de ses activités.

L'article 16 LCPD assimile certes à des autorités les mandataires externes appelés à traiter des données personnelles dans le cadre de leur mandat. Ces mandataires doivent néanmoins s'engager contractuellement à appliquer les mesures prévues par la présente loi lorsqu'ils traitent des données non personnelles. Tout mandataire a l'obligation de surveiller ses réseaux. Il doit repérer toute anomalie, agression et panne suffisamment tôt, les évaluer et les signaler au donneur d'ordre, afin que celui-ci puisse réagir. En cas de suspicion de danger ou de violation avérée de la sécurité de l'information et de la cybersécurité, il est parfois nécessaire de contrôler en détail les activités numériques de certaines collaboratrices et collaborateurs internes ou externes (ou de leur machine). Les dispositions de l'ordonnance sur les données secondaires de communication (ODSC)[20] portant sur traitement de données personnelles dans le cadre de l'utilisation de l'infrastructure informatique s'appliquent si ce contrôle nécessite l'identification nominative d'une personne.

8.5 Mesures physiques

Article 13 – Principe

Les mesures de protection physique visent à réduire les risques de destruction. Parmi ces risques figurent notamment des actes humains (p. ex. espionnage, vol, vandalisme ou sabotage), mais aussi les dommages pouvant être causés par des éléments naturels (p. ex. chaleur, feu, eau, poussière, vibrations, etc.). L'article 13 pose le principe selon lequel les autorités doivent garantir la protection physique de leurs informations et outils TIC. Elles doivent en particulier empêcher tout accès non autorisé aux informations et aux outils TIC, par exemple grâce à des contrôles d'accès, des dispositifs de vidéosurveillance, des systèmes de verrouillage, du mobilier de sécurité, des appareils de destruction de documents, etc. Parmi les dispositifs contre les risques que présentent les éléments naturels figurent notamment les alarmes incendies et les extincteurs automatiques. Des mesures de protection

[20] ODSC, RSB 153.011.5 : https://www.belex.sites.be.ch/app/fr/texts_of_law/153.011.5/versions/1781

physique doivent être prises tant pour les informations et les outils TIC qui se trouvent dans les locaux de l'autorité ou de l'organisation que pour ceux dont l'accès est public. Dans ce dernier cas, il s'agit des informations et outils TIC devant pouvoir être utilisés ailleurs qu'à leur emplacement usuel (bureau) et protégés en dehors du périmètre de sécurité habituel, par exemple au domicile en cas de télétravail. Mais il peut aussi s'agir d'informations, d'équipements, de câblages et de circuits d'alimentation qui ne sont pas sous le contrôle permanent de l'autorité ou de l'organisation. Il faut être particulièrement vigilant aux points d'accès, comme les zones de livraison et de chargement.

Article 14 – Zones de sécurité

La transformation de certaines salles ou secteurs en zone de sécurité constitue une mesure physique de sécurité de l'information et de cybersécurité que la police et l'Office de l'exécution judiciaire (OEJ) ont déjà mise en place, surtout pour protéger les salles de serveur, de travail ou les salles de gestion des interventions. Toute zone de sécurité doit être prédéfinie, identifiable comme telle et protégée en conséquence. Elle peut se composer de quelques salles, de tout un ensemble de salles ou d'un bâtiment entier. Les mesures devront y être mises en place en fonction des risques. L'autorité se base sur eux pour déterminer son équipement effectif.

L'alinéa 2 règle les prérogatives particulières de l'autorité ou de l'organisation créant une zone de sécurité :

- Elle peut restreindre l'introduction de certains objets dans les zones de sécurité. En règle générale, il n'est possible d'y faire entrer des appareils d'enregistrement d'images ou de son (y compris les smartphones et les ordinateurs portables équipés de ce genre de dispositifs) qu'avec une autorisation spéciale.

- Les secteurs de la zone de sécurité particulièrement importants pour la sécurité de l'information et la cybersécurité (p. ex. l'entrée d'une salle de serveur, le bureau de l'administrateur ou la salle d'archivage d'informations classifiées « SECRET ») peuvent être surveillés grâce à des dispositifs d'enregistrement vidéo. L'installation d'un dispositif de vidéosurveillance et le délai de conservation des enregistrements (qui devra être réglé par voie d'ordonnance) doivent être proportionnés (cf. « Explications sur la vidéosurveillance sur le lieu de travail » du préposé fédéral à la protection des données et à la transparence (PFPDT)[21].

- L'autorité peut faire contrôler les sacs et les personnes à l'entrée et à la sortie de la zone, afin d'éviter que des appareils y soient introduits sans autorisation ou que des informations soient dérobées (copiées sur une clé USB par exemple). La fouille des poches, à titre de mesure de sécurité légitime basée sur l'existence d'un risque, doit reposer sur un mobile précis. En outre, elle doit, en principe, être annoncée et mise à exécution de manière proportionnée[22].

- Pour appliquer les dispositions, il doit également être possible de contrôler les bureaux, afin surtout de vérifier que la politique dite « du bureau propre » est bien appliquée : aucune information digne de protection ne doit traîner sur les bureaux ou ailleurs, les ordinateurs doivent être verrouillés ou éteints, les supports de données doivent être rangés dans un endroit fermé à clé, les tiroirs doivent être fermés, les corbeilles à papier ne doivent contenir aucune information classifiée, etc. Ces contrôles peuvent également avoir lieu en l'absence des personnes concernées, par exemple la nuit.

- Dans les zones de sécurité particulièrement sensibles, l'autorité peut placer des installations perturbatrices. L'utilité effective et les conditions d'utilisation de ces brouilleurs doivent être évaluées conformément à la loi fédérale sur les télécommunications (LTC).

[21] Disponible à l'adresse https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/arbeitsbereich/surveillance-sur-le-lieu-de-travail/explications-sur-la-videosurveillance-sur-le-lieu-de-travail.html (consultée le 8.1.2023 pour la dernière fois)
[22] Cf. Stefanie Meier-Gubser, *Mirarbeiterüberwachung : Rechte, Pflichten und Verbote,* TREX 2020, p. 286 à 291 (en allemand)

8.6 Mesures concernant les personnes

8.6.1 Sélection, formation et habilitation

Article 15 – Conditions d'accès aux informations et aux outils TIC

Toute personne ayant accès à des informations, des outils TIC ou des infrastructures des autorités doit satisfaire à certaines exigences. Il appartient à l'autorité de s'assurer que ses employé·e·s et ses mandataires les remplissent.

a. Les personnes devant être engagées ou devant exécuter un mandat doivent être sélectionnées selon des critères correspondant au besoin de protection des informations et à la criticité des outils TIC. Les autorités répondent des personnes qu'elles engagent. Le fait de soumettre une personne à un CSP ne les dégage pas de cette responsabilité.

b. L'administration des accès aux systèmes d'information, aux locaux et aux infrastructures est de plus en plus informatisée. Les personnes qui veulent accéder aux outils TIC des autorités doivent apporter la preuve de leur identité (procédure d'authentification) pour pouvoir en obtenir les droits d'accès. Les systèmes d'authentification peuvent être plus ou moins renforcés selon la criticité de l'accès, par exemple au moyen d'une carte à puce ou d'un contrôle biométrique (par reconnaissance des empreintes digitales, de l'œil, etc. ; cf. art. 31, al. 2, lit. *c* LAN).

c. Les autorités doivent fournir une formation suffisante aux personnes qu'elles emploient et à leurs mandataires. En matière de sécurité de l'information et de cybersécurité, une seule formation ne suffit pas. Le personnel et les mandataires doivent être régulièrement sensibilisés au sujet et formés dans ce domaine. La formation du personnel d'encadrement et des autres personnes exerçant une activité sensible au plan de la sécurité est particulièrement importante.

   Les personnes employées par les autorités doivent respecter le secret de fonction en application de l'article 58 LPers et de l'article 320 du Code pénal suisse (CP)[23]. Tout mandat confié à un tiers doit spécifier que celui-ci exerce temporairement des fonctions officielles en qualité d'auxiliaire et qu'il est à ce titre soumis au secret de fonction. Cette disposition a été clarifiée dans le cadre de la révision de l'article 320 CP concomitante à l'élaboration de la LSI.

Article 16 – Habilitation restrictive

Cette disposition formule un principe capital en matière de sécurité de l'information et de cybersécurité. Toute personne travaillant ou exécutant un mandat pour une autorité peut être appelée dans certaines circonstances à utiliser certaines informations, des outils TIC ou des locaux pour accomplir sa mission. Il est primordial de ne lui octroyer que les droits d'accès dont elle a effectivement besoin pour exécuter sa tâche. On réduit considérablement le risque d'utilisation abusive en l'empêchant de traiter sans motif des informations d'un autre domaine.

Il n'est pas rare qu'au terme de leur contrat de travail ou de leur mandat, les employé·e·s ou les mandataires ne soient pas enjoints de restituer leur clé ou leur badge ou que leur compte d'utilisateur ne soit pas bloqué. Leurs droits d'accès, qui ne sont plus valables, peuvent alors être utilisés contre les intérêts de leur ancien employeur ou donneur d'ordre. Il faut donc veiller à retirer les droits d'accès à la fin d'un engagement ou d'un mandat. Ils doivent être bloqués ou supprimés dès qu'il y a des raisons de craindre que la sécurité de l'information et la cybersécurité sont menacées. L'objectif principal de ces deux mesures est de réduire le risque d'un acte interne.

[23] CP, RS 311.0 : https://www.fedlex.admin.ch/eli/cc/54/757_781_799/fr

8.6.2 Contrôle de sécurité relatif aux personnes (art. 17 à 19)

La règlementation des contrôles de sécurité relatifs aux personnes (CSP) confère à toutes les autorités une base légale expresse leur permettant de contrôler la probité des candidats et candidates à l'embauche, du personnel en poste et des tiers mandatés exerçant une activité touchant à la sécurité (comme le personnel d'encadrement ou les administrateurs de systèmes). Ces contrôles permettent en particulier aux autorités de constater qu'une personne a des antécédents judiciaires entachant sa probité ou qu'elle a des dettes qui en font une cible de chantage. Grâce à ces mesures d'organisation, les autorités peuvent réduire le risque que des membres du personnel causent intentionnellement des failles de sécurité. Il incombe à chaque autorité de désigner, sur la base de son évaluation des risques (art. 5, al. 4), les personnes qu'elle veut soumettre à un CSP et de déterminer la fréquence de ces contrôles.

À la place du CSP relativement compliqué et fastidieux que prévoit le droit fédéral (art. 27 à 48 LSI), la LSIC adopte, avec quelques adaptations minimes, la réglementation de la loi sur la police d'ores et déjà en vigueur dans la Police cantonale (art. 149, al. 4 et art. 160 à 162 LPol). Conformément à ces dispositions, les CSP ne sont pas réalisés, comme dans l'administration fédérale, par un service spécialisé ad hoc, mais par chaque autorité elle-même, qui exige dans la plupart des cas un extrait du casier judiciaire ou du registre des poursuites. Le rapport relatif à la révision totale de la LPol fournit toutes les explications à ce sujet[24]. La LSIC apporte les adaptations suivantes à cette réglementation :

- L'article 17, alinéa 1 formalise l'objectif du CSP.

- Aux termes de l'article 17, alinéa 2, outre les personnes employées (art. 160 LPol) et les mandataires (art. 149, al. 4 LPol), les membres d'autorités qui sont désignés par voie d'élection (juges, procureur·e général·e) peuvent aussi être soumis à un CSP avant leur élection. Pour les personnes élues par le Grand Conseil, l'organe compétent pour réaliser un CSP est la Commission qui prépare l'élection et soumet une proposition de vote et, pour les personnes élues par le Conseil-exécutif, la Direction demandeuse. Faute d'autorité élective, il est impossible de soumettre à un CSP les membres d'autorités qui sont élus par le peuple, comme les parlementaires, les conseillers et conseillères d'État ainsi que les préfets et préfètes.

- L'article 17, alinéa 3 étend les conditions de réalisation d'un CSP par rapport à celles que prévoit la LPol. Ce contrôle n'est pas réservé aux cas (spécifiques à la police) énumérés de manière exhaustive ; il peut aussi être réalisé lorsqu'il constitue une mesure de protection adéquate contre le risque de sécurité que présente le recours à la personne à contrôler. Cette règle correspond à l'approche axée sur le risque fondant la LSIC. C'est à l'autorité responsable d'évaluer ce risque dans le cadre de ses fonctions de gestion des risques (art. 5, al. 4). L'article 17, alinéa 3 reprend à titre illustratif les cas d'application prévus par la LPol et les étend : il autorise désormais un CSP lorsque la personne à contrôler est appelée, dans le cadre de son activité, à avoir fréquemment accès à des informations classifiées ou à des données personnelles particulièrement dignes de protection ou à un volume important d'éléments de ce type, à consulter d'importants dossiers politiques ou affaires de sécurité, sur lesquels elle peut ainsi exercer une influence, ou à avoir accès, régulièrement ou sans accompagnement, à des installations ou à des locaux présentant un risque de sécurité ou à des zones de sécurité au sens de l'article 14.

- L'article 17, alinéa 5 établit clairement que les personnes soumises à un CSP en vertu du droit fédéral y restent soumises.

- L'article 18, alinéa 2 ne reprend pas le registre des bureaux du contrôle des habitants comme source de données du CSP (art. 161, al. 2, lit. *c* LPol), car on ne voit pas bien quelles données importantes pour la sécurité il peut contenir. Il cite à la place (explicitement) le casier judiciaire,

[24] Rapport relatif à la LPol, p. 74 et suivante

afin d'établir clairement que les autorités peuvent réclamer un extrait de casier judiciaire dans le cadre du CSP. Toute autre autorité que la Police cantonale souhaitant exceptionnellement avoir accès aux fichiers de données spécifiques à la police conformément aux articles 143 et 147 LPol doit en faire la demande à la Police cantonale en actionnant l'assistance administrative. La Police cantonale n'est pas tenue de lui répondre favorablement. Elle n'accèdera à ces demandes que s'il est établi qu'un extrait de casier judiciaire ou du registre des poursuites ne suffit pas.

- Aux termes de l'article 19, alinéa 2, les résultats du CSP ne doivent être communiqués aux personnes contrôlées que s'ils sont négatifs, afin de limiter la charge administrative.

Ces dispositions appellent en outre les remarques suivantes :

- Article 19, alinéa 2 : la procédure de rectification de données inexactes est définie par la législation sur la protection des données (art. 23 LCPD).

- Article 19, alinéa 3, lettre *b* : la possibilité de revenir sur une promesse écrite peut également être prévue sous forme de clause suspensive insérée dans le contrat de travail. Il est toutefois préférable de n'établir ce dernier qu'après avoir procédé au CSP et, en cas de promesse préalable, de la délivrer sous réserve expresse du résultat du CSP.

- Le CSP et ses effets devront être réglés en détail par voie d'ordonnance. Ce texte devra par exemple établir que quiconque refuse de se plier à un CSP encourt les retombées prévues par la législation sur le personnel, comme de ne pas être engagé ou d'être muté à une fonction moins sensible voire, si cette mutation est impossible, d'être licencié.

- Étant donné qu'il est impossible pour l'instant d'estimer la charge que représente, pour la Police cantonale, le fait d'avoir à apporter son concours aux CSP, il est prévu de n'édicter les réglementations nécessaires par voie d'ordonnance ou d'instruction qu'après une année d'expérimentation, de sorte à réduire la charge de la Police cantonale à un niveau acceptable si cela s'avère nécessaire.

8.7 Organisation de la sécurité

Actuellement, la sécurité de l'information du canton est organisée au coup par coup et le plus souvent par domaine. Comme sa garantie est une fonction de direction permanente exercée par le Conseil-exécutif et par l'administration, la LSIC donne un socle à une organisation supradirectionnelle, commune à tous les domaines spécialisés de l'administration. L'objectif est de renforcer l'attention que les instances dirigeantes portent aux affaires de sécurité et la sensibilisation des spécialistes et du personnel d'encadrement de l'administration en la matière.

Article 20 – Organisation de la sécurité des autorités cantonales au sens de l'article 2, alinéa 1

Avec la loi et l'ordonnance sur l'administration numérique (LAN et OAN[25]), le Conseil-exécutif a créé des organes assurant le pilotage et la gestion de la transformation numérique et des TIC tant pour le canton dans son ensemble (y compris pour les affaires des communes et des organisations autonomes chargées de tâches publiques) que pour l'administration cantonale. Étant donné que les questions de sécurité de l'information se posent avant tout en relation avec les systèmes TIC et les projets de numérisation, la LSIC prévoit que l'organisation de la sécurité cantonale soit intégrée aux organes institués par la LAN et l'OAN. Cela facilite la prise en compte de la sécurité comme composante de la transformation numérique de l'administration publique et évite d'avoir à instituer de nouveaux organes spécialisés.

[25] www.be.ch/lan

À l'avenir, les organes administratifs suivants assureront aussi des tâches de sécurité : l'organe de contact canton-communes pour la numérisation (OCCCN), chargé des échanges politiques entre le canton et les communes, ainsi que la Conférence pour l'administration numérique et les TIC (CNT) et son groupe spécialisé Sécurité de l'information, qui élaborent et édictent des règles de sécurité (instructions, normes et processus par exemple). L'article 20, alinéa 3 LSIC reprend la règle déjà prévue par la LAN et l'OAN selon laquelle les communes doivent être associées de manière appropriée aux décisions des organes cantonaux qui les concernent.

Article 21 – Organisation de la sécurité des communes et des autres organisations chargées de tâches publiques au sens de l'article 2, alinéa 2

Les autorités qui n'appartiennent pas à l'administration cantonale doivent se doter d'une organisation de sécurité adaptée à leurs tâches et à leurs risques. Parmi elles figurent toutes les organisations chargées de tâches publiques qui ne sont pas hiérarchiquement subordonnées au Conseil-exécutif, comme le Grand Conseil, les autorités de justice, les établissements cantonaux autonomes, les entreprises publiques, les communes et les organisations chargées de tâches communales.

Ces autorités doivent désigner au moins une personne dotée de compétences et de ressources appropriées, qui jouera également le rôle d'interlocutrice des autorités cantonales et fédérales en matière de sécurité. Les communes ou autorités de moindre envergure peuvent instituer une personne commune ou confier cette responsabilité à un ou une spécialiste externe.

8.8 Dispositions finales

Article 22 – Dispositions d'exécution

À l'instar de l'article 34 LAN, la LSIC permet de déléguer aux organes de l'administration cantonale compétents en la matière (cf. art. 20 LSIC) le soin d'édicter des dispositions d'exécution techniques ainsi que des règles de mise en œuvre de la LSIC. Les dispositions édictées par ces organes ne constituent pas des ordonnances législatives, mais des instructions (prescriptions administratives) à l'attention d'autres autorités.

Les délais transitoires nécessaires à la mise en œuvre de la loi doivent être fixés par voie d'ordonnance. Il s'agit notamment de définir des délais appropriés pour la première classification de toutes les informations ainsi que pour l'adaptation des systèmes TIC et de l'organisation en fonction de la LSIC et des consignes de sécurité qui en découlent. Les organes spécialisés compétents détermineront ces délais et élaboreront la procédure de mise en place en concertation avec les autorités concernées.

Article 23 – Modification d'autres actes

Dans la loi sur la police, les dispositions relatives au contrôle de sécurité relatif aux personnes (art. 17, al. 4, 149, al. 4 et 160 à 162) sont abrogées, car elles sont transférées aux articles 17 à 19 LSIC.

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

La présente loi s'inscrit dans le programme gouvernemental de législature 2023 à 2026, qui prévoit, comme deuxième objectif, que le canton de Berne recoure à la transformation numérique pour fournir des services à la fois efficaces, économiques et de grande qualité. La qualité de ces services implique qu'ils soient sécurisés, car c'est la garantie que la population et les acteurs économiques soient disposés à confier leurs données personnelles et leurs informations à caractère confidentiel aux autorités.

La présente loi s'inscrit également dans la Stratégie pour une administration numérique que le Conseil-exécutif a arrêtée en 2019 (cf. points 2.2 et 3.2.2.2 plus haut).

10. Répercussions financières

La loi doit en principe être mise en œuvre avec les moyens financiers existants et planifiés, prévus pour les TIC et la numérisation. Et ce pour les raisons suivantes :

- Les autorités ont d'ores et déjà l'obligation de garantir la sécurité des données conformément à l'article 17 de la loi sur la protection des données (LCPD). La LSIC n'instaure donc pas de nouvelle tâche étatique, mais elle concrétise seulement une tâche existante.

- La numérisation de l'administration est certes un inducteur de coûts pour les TIC et donc pour la sécurité de l'information et la cybersécurité, particulièrement dans le contexte des menaces croissantes qui pèsent sur la cybersécurité. Mais la LAN et la LSIC mettent dans les mains des autorités responsables plusieurs outils qui leur permettent de réduire ou de compenser les surcoûts relatifs aux TIC et à la sécurité:

    - La numérisation résolue et l'intensification de l'automatisation des processus d'affaires impliquant des échanges avec les autorités, les entreprises et les professionnels (cf. art. 8 LAN) permettront de réduire les coûts de matériel et de personnel (pour le traitement des dossiers, le secrétariat, la saisie des données, le port, le papier et l'impression, etc.).

    - Si des autorités collaborent à la numérisation (art. 20 LAN), par exemple en acquérant et en exploitant ensemble des systèmes communs à plusieurs cantons ou communes ou en utilisant les services de base cantonaux existants (art. 16 s. LAN), elles pourront fortement réduire, voire éviter les coûts de sécurité liés à la numérisation.

    - Si les autorités appliquent une gestion des risques appropriée (art. 5, al. 4 LSIC), elles peuvent cibler leurs mesures de sécurité sur les aspects de leur activité qui présentent le plus de risques et tolérer sciemment les risques dans des domaines moins sensibles (art. 11, al. 2, lit. *d* LSIC). Si elles se bornent à classifier uniquement les informations nécessaires (art. 8, al. 3 LSIC), elles réduisent le nombre de systèmes avec échelon de sécurité élevé (art. 11, al. 2, lit. *b* LSIC) et, par conséquent, les coûts qui en résultent.

11. Répercussions sur le personnel et l'organisation

Du fait de la situation financière et de la politique en matière de personnel, la législation sur la sécurité de l'information devra en principe être mise en œuvre dans l'administration cantonale avec les ressources en personnel existantes. Nous renvoyons à ce sujet aux explications données ci-dessus au chiffre 10. Les répercussions sur le personnel seront également restreintes du fait que les organes

spécialisés dans la sécurité de l'information seront intégrés dans l'actuelle gouvernance de l'administration numérique et des TIC (cf. art. 20 LSIC).

12. Répercussions sur les communes et les autres organisations chargées de tâches publiques

Si la tâche concernant la sécurité de l'information n'est pas nouvelle pour le canton, elle ne l'est pas non plus pour les communes et les autres organisations chargées de tâches publiques (art. 17 LCPD). Mais la LSIC ne s'applique à elles que dans la mesure, limitée, où elles interagissent avec le canton ou la Confédération, plus précisément avec leurs systèmes et leurs informations (art. 2, al. 2 LSIC). Elles doivent dans ce contexte respecter les règles régissant la classification et le maniement des informations classifiées et des systèmes TIC.

Les communes et les autres organisations chargées de tâches publiques sont par ailleurs libres de se doter de leurs propres règles en matière de sécurité de l'information ou d'adopter toutes celles de la LSIC, ce qui aurait l'avantage de créer un espace de sécurité uniforme dans le canton de Berne. Elles peuvent elles aussi maîtriser les coûts de la sécurité de l'information en arrêtant des mesures de sécurité ciblées et adaptées aux risques et en créant des synergies avec d'autres communes et avec l'administration cantonale.

13. Répercussions sur l'économie

L'évaluation réalisée à l'aide de la check-list pour l'analyse d'impact de la réglementation a montré que le présent projet n'a pas de répercussions notables sur les charges administratives ou financières des entreprises ni sur l'économie dans son ensemble.

14. Résultat de la procédure de consultation

15. Proposition

Le Conseil-exécutif propose au Grand Conseil d'adopter la présente loi.