Rapport

Date de la séance du CE : 9 septembre 2026
Direction : Direction des finances
Numéro d'affaire : 2023.KAIO.444
Classification : Non classifié

Ordonnance sur la sécurité de l'information et des données (OSID)

Sommaire

1. Synthèse 2

2. Contexte 2
2.1 Confédération 2
2.2 Canton de Berne 3
2.2.1 Lois 3
2.2.2 Ordonnances et instructions 3
2.3 Besoin d'améliorations 4

3. Caractéristiques de l'OSID 5
3.1 Hiérarchie et architecture des normes 5
3.2 Niveaux de protection 6
3.3 Synthèse du contenu 7
3.4 Organisation de la sécurité du canton et de l'administration cantonale 7
3.5 Objectifs d'effet 9

4. Forme de l'acte législatif 9

5. Droit comparé 10
5.1 Confédération 10
5.2 Cantons 10

6. Mise en œuvre et évaluation 10

7. Commentaire des articles 10
7.1 Dispositions générales 10
7.2 Principes de la sécurité de l'information et des données 12
7.3 Mesures de protection des autorités cantonales 24
7.3.1 Procédure de sécurité applicable aux outils TIC 24
7.3.2 Gestion de la sécurité de l'information et des données 27
7.3.3 Classification d'informations 32
7.3.4 Détermination du besoin de protection des outils TIC 36
7.3.5 Personnes à contrôler 36
7.4 Organes chargés de la sécurité 37
7.5 Dispositions transitoires et finales 44

8. Place du projet dans le programme gouvernemental de législature et dans d'autres planifications importantes 46

9. Répercussions sur les finances, l'organisation, le personnel, l'informatique et les locaux 47
9.1 Sécurité de l'information 47
9.2 Sécurité des données 48

10. Répercussions sur les communes et les autres organisations chargées de tâches publiques 48
10.1 Sécurité de l'information 48
10.2 Sécurité des données 49

11. Répercussions sur l'économie 49

12. Proposition 50

1. Synthèse

L'ordonnance sur la sécurité de l'information et des données (OSID)[1] contient les dispositions d'exécution de la loi du 12 juin 2025 sur la sécurité de l'information et la cybersécurité (LSIC)[2] ainsi que les dispositions d'exécution de la loi cantonale sur la protection des données (LCPD)[3], entièrement révisée, relatives à la sécurité des données. Elle s'inspire en outre de l'ordonnance du 8 novembre 2023 sur la sécurité de l'information dans l'administration fédérale et l'armée (ordonnance sur la sécurité de l'information, OSI)[4], en l'adaptant toutefois au contexte bernois et en n'en reprenant donc que le minimum.

L'OSID précise à l'intention de l'ensemble des autorités bernoises les principes et les mesures de protection applicables à la sécurité de l'information et des données prévus par la LSIC et la LCPD. Par rapport aux autres autorités, en particulier les communes municipales, les paroisses et les communes bourgeoises, la législation impose aux autorités cantonales des règles supplémentaires destinées à permettre à la Confédération de reconnaître leur équivalence, de sorte qu'elle continue à collaborer sans réserve avec le canton de Berne dans des domaines critiques pour la sécurité.

L'OSID remplace l'ordonnance de Direction du 3 janvier 2011 concernant la sûreté de l'information et la protection des données (OD SIPD)[5]. Elle intègre en outre toutes les dispositions relatives à la sécurité des données de l'actuelle ordonnance du 22 octobre 2008 sur la protection des données (OPD)[6], renommée « ordonnance cantonale sur la protection des données » (OCPD) depuis la révision de la LCPD.

Les mesures de protection étant les mêmes pour la sécurité de l'information que pour celle des données, elles sont regroupées et uniformisées dans l'OSID. L'OSID entrera en vigueur à la même date que la LSIC, soit le 1er novembre 2026.

2. Contexte

2.1 Confédération

Depuis l'entrée en vigueur de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information (loi sur la sécurité de l'information, LSI)[7] le 1er janvier 2024, les cantons sont tenus, lorsqu'ils accèdent à des outils TIC, à des informations ou à des données personnelles de la Confédération, soit d'appliquer directement les dispositions fédérales soit de garantir une sécurité au moins équivalente de l'information (art. 3 LSI).

Également en vigueur depuis le 1er janvier 2024, l'OSI définit non seulement les dispositions d'exécution concernant notamment la gestion de la sécurité de l'information et les mesures de protection organisationnelles, techniques, physiques et celles relatives au personnel, mais aussi les organes chargés de la sécurité ainsi que leurs responsabilités et compétences (art. 36 ss OSI). Vu l'importance fondamentale de cette ordonnance pour l'équivalence de la sécurité de l'information des cantons requise par la Confédération au sens de l'article 3 en relation avec l'article 86 LSI, l'OSID s'en inspire pour garantir que le canton de Berne satisfasse aux exigences de la Confédération – largement adaptées au contexte bernois et réduites.

[1] OSID, RSB 152.091
[2] LSIC, RSB 152.09
[3] LCPD, RSB 152.04
[4] OSI, RS 128.1
[5] OD SIPD, RSB 152.040.2
[6] OPD, RSB 152.040.1
[7] LSI, RS 128

Le 1er avril 2025, la Confédération a par ailleurs promulgué l'ordonnance du 7 mars 2025 sur la cybersécurité (ordonnance sur la cybersécurité, OCyS)[8], qui concrétise notamment l'obligation faite aux exploitantes et exploitants d'infrastructures critiques de signaler les cyberattaques. L'OSID vise à simplifier sensiblement les obligations de signaler que les LSIC, LCPD et OCyS imposent aux autorités bernoises et à les coordonner grâce à une plateforme unique.

2.2 Canton de Berne

2.2.1 Lois

Les quatre lois cantonales bernoises, déjà en vigueur, régissant les principes de la sécurité de l'information et des données ainsi que de la protection des données sont les suivantes :

a) Loi du 10 mars 2020 sur les fichiers centralisés de données personnelles (LFDP)[9], entrée en vigueur le 1er mars 2021
b) Loi du 7 mars 2022 sur l'administration numérique du canton de Berne (LAN)[10], entrée en vigueur le 1er mars 2023
c) Loi révisée sur la protection des données (LCPD), entrée en vigueur le 1er septembre 2026
d) Loi sur la sécurité de l'information et la cybersécurité (LSIC), adoptée à l'unanimité par le Grand Conseil en seconde lecture le 12 juin 2025 et entrée en vigueur à la même date que l'OSID, soit le 1er novembre 2026

C'est sur ces quatre piliers que reposent la sécurité de l'information et des données ainsi que la protection des données (« Quatre piliers de la SIPD ») :

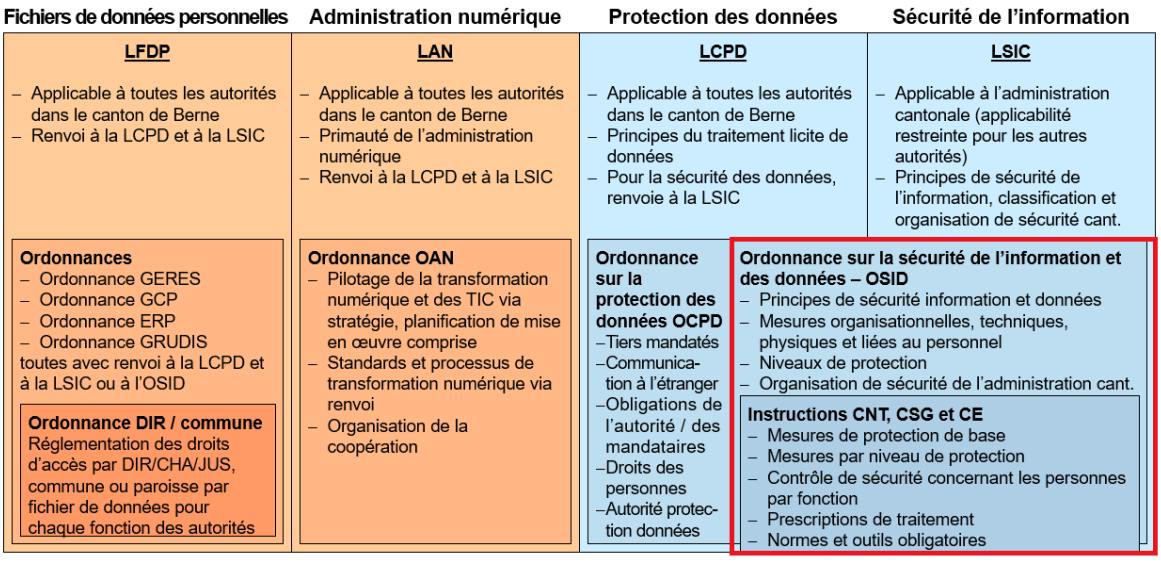


Illustration 1 : Les « quatre piliers de la SIPD » de la législation bernoise

2.2.2 Ordonnances et instructions

Depuis l'instauration de la LCPD, en 1986, le canton de Berne a édicté, dans le cadre de la transformation numérique de la gestion publique, de nombreuses ordonnances et instructions destinées

[8] OCyS, RS 128.51
[9] LFDP, RSB 152.05
[10] LAN, RSB 109.1

à protéger les données personnelles dans un premier temps, puis les informations critiques pour la gouvernance étatique. Parmi elles figurent notamment les textes suivants :

a) Ordonnances

1. Ordonnance du 22 octobre 2008 sur la protection des données (OPD)
2. Ordonnance de Direction du 3 janvier 2011 concernant la sûreté de l'information et la protection des données (OD SIPD)
3. Ordonnance du 13 mars 2013 sur la classification, la publication et l'archivage des documents relatifs aux affaires du Conseil-exécutif (ordonnance sur la classification, OCACE)[11]
4. Ordonnance du 20 novembre 2019 sur les données secondaires de communication (ODSC)[12]
5. Ordonnance du 11 janvier 2023 sur l'administration numérique (OAN)[13]

b) Instructions et directives

1. Directives du Conseil-exécutif du 24 novembre 2021 sur la gestion des risques du canton de Berne (Directives GR)[14]
2. Directive du Conseil-exécutif du 17 mars 2021 sur l'utilisation de programmes de traduction automatique en ligne dans l'administration cantonale[15]
3. Instruction de la Conférence pour l'administration numérique et les TIC (CNT)[16] régissant l'utilisation des comptes et des ID utilisateur·trice[17]
4. Instruction du Comité stratégique TIC (CST) sur les normes relatives aux technologies de l'information et de la communication dans l'administration cantonale (normes TIC BE) du 8 décembre 2020[18]
5. Instruction de la CNT régissant l'emploi des TIC dans l'administration cantonale applicable aux utilisateurs et utilisatrices finales du 27 juin 2023[19]
6. Instruction de l'OIO régissant la sécurité des réseaux (Network Security Policy, NSP) du 18 décembre 2024[20]
7. Instruction de l'OIO sur la gestion des identités et des accès (IAM) et sur les services d'annuaire (instruction IAM) du 4 mars 2024[21]
8. Instruction de l'OIO sur la protection de base en matière de sécurité de l'information et de cybersécurité (IPSIC) du 9 juillet 2025[22]

2.3 Besoin d'améliorations

Il suffit d'un coup d'œil pour constater que les réglementations, les champs d'application et, surtout, les responsabilités des différentes autorités en matière de sécurité de l'information et des données manquent d'harmonisation et de systématique. Ce défaut s'explique principalement par l'évolution constante, rapide et spontanée des outils TIC depuis 1986 et, avec elle, des exigences concernant le développement des démarches numériques au sein de la population et de l'administration. Les exigences ont également changé en ce qui concerne la législation, qui a eu des difficultés à suivre les progrès techniques en raison de la multitude de questions devant être réglées dans une loi ou une ordonnance, dont l'élaboration prend du temps.

[11] OCACE, RSB 152.17
[12] ODSC, RSB 153.011.5
[13] OAN, RSB 109.111
[14] ACE 1382/2021
[15] Directive sur les programmes de traduction automatique en ligne à la page Référentiel AN et TIC (interne à l'administration)
[16] Art. 18 OAN
[17] Instruction régissant les ID utilisateur·trice à la page Référentiel AN et TIC
[18] Normes TIC BE à la page Référentiel AN et TIC
[19] Instruction applicable aux utilisateurs et utilisatrices à la page Référentiel AN et TIC
[20] Instruction NSP-BE à la page Référentiel AN et TIC (en allemand)
[21] Instruction IAM à la page Référentiel AN et TIC
[22] IPSIC

Avec les textes désignés ci-avant formant les « quatre piliers de la SIPD », le canton de Berne s'est doté d'objectifs stratégiques permettant une réorganisation à la fois systématique et réactive de la sécurité de l'information et des données ainsi que de la protection des données.

Lors de l'élaboration de la LSIC, le législateur s'est donc penché sur les réglementations susmentionnées afin de déterminer lesquelles devaient être conservées, abrogées, déléguées ou reprises. Cet examen se poursuivra au niveau des instructions. La hiérarchie des normes ci-après joue un rôle essentiel à cet égard.

3. Caractéristiques de l'OSID

3.1 Hiérarchie et architecture des normes

La LSIC et la LCPD révisée forment ensemble la base d'un dispositif réglementaire complet de pilotage et de gestion de la sécurité de l'information et des données du canton de Berne. Prenant appui sur les normes à caractère général et abstrait de la LSIC et de la LCPD, ce dispositif s'étend de l'OSIC 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 :

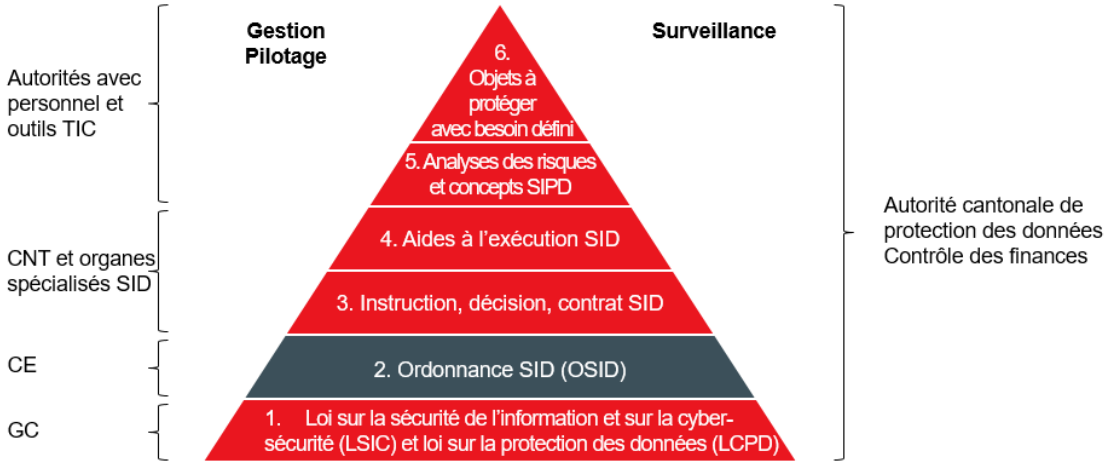


Illustration 2 : Hiérarchie des normes relatives à la sécurité de l'information et des données (SID)

Alors que le rapport du 16 août 2023 relatif à la LSIC indiquait, au chiffre 4.2, que la hiérarchie des normes reposait uniquement sur ladite loi, elle s'appuie dorénavant aussi sur la LCPD révisée. Cela s'explique par le fait que l'OSID fonde la sécurité de l'information mais aussi celle des données. Pour garantir la sécurité des informations et des données personnelles, il est impératif d'assurer leur intégrité, leur disponibilité, leur confidentialité et la traçabilité de leur traitement.

La sécurité de l'information est définie à l'article 4, alinéa 1, lettre *a* LSIC et celle des données à l'article 10, alinéa 2 LCPD, qui renvoie à la LSIC. Toutes deux constituent les conditions préalables devant être remplies pour que les informations et les données personnelles soient traitées conformément à la LSIC et à la LCPD et, partant, dans le respect du droit.

3.2 Niveaux de protection

Les conditions préalables sont réputées remplies lorsque les mesures de protection déterminées en fonction des risques sont mises en œuvre. Ces mesures étant identiques pour la sécurité de l'information et la sécurité des données, elles sont désignées dans la LSIC par le terme générique « niveaux de protection », qui vont de 0 à 3. La CNT édicte une instruction régissant les mesures de protection que doivent prendre les autorités cantonales pour garantir les niveaux de protection 0 et 1, c'est-à-dire la protection de base, des objets à protéger du canton et de ceux de la Confédération. Si les autorités cantonales mettent des objets à protéger à la disposition de tiers, elles définissent les mesures de protection correspondantes dans une instruction, une décision ou un contrat et délèguent leur mise en œuvre à ces tiers. Par ailleurs, les responsables de la sécurité des autorités chargées des objets à protéger arrêtent les mesures de protection nécessaires pour réduire le risque en matière de sécurité au niveau qu'ils ont accepté.

L'OSID constitue ainsi une interface entre la LSIC et la LCPD.

Loi sur la sécurité de l'information et la cybersécurité - LSIC		**Ordonnance sur la sécurité de l'information et des données - OSID**	**Loi sur la protection des données – LCPD**
Protection des intérêts de l'État		**Mesures relatives à la sécurité de l'information et des données**	**Protection des intérêts des personnes physiques**
Outils TIC	Informations	Mesures de protection selon l'évolution de la technique	Données personnelles
Protection très élevée	SECRET	Niveau de protection 3	Données personnelles représentant une grave menace pour la sécurité de la personne concernée (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)
Contrôle de sécurité concernant des personnes (CSP) au sens de la LSIC par autorité responsable de l'engagement		Dispositions d'exécution pour la LSIC et la LCPD	Contrôle de la probité des personnes selon la loi sur le personnel par l'autorité responsable de l'engagement

Illustration 3 : Objets à protéger, besoins de protection et niveaux de protection selon l'OSID : « interface » entre la LSIC et la LCPD

Il est important de bien distinguer les objectifs de protection ou les objets à protéger de la LSIC de ceux de la LCPD :

- la LSIC protège des intérêts publics comme la liberté de décision, la capacité d'action et l'accomplissement des tâches de l'État ;
- la LCPD protège des intérêts privés, à savoir des personnes contre des atteintes illicites à leur personnalité.

Au vu de ces différences d'intérêts, les deux lois ont établi leurs propres définitions du besoin de protection (voir première, deuxième et quatrième colonnes de l'illustration 3), que l'OSID harmonise par le biais des quatre niveaux de protection (troisième colonne). Bien que les objectifs de protection divergent, les mesures de protection sont les mêmes.

Le besoin de protection d'une information, d'une donnée personnelle ou d'un outil TIC est défini en fonction de son importance, et de cette définition découle le niveau de protection. Chaque niveau de protection correspond à l'ensemble des mesures de protection organisationnelles, techniques, physiques ou liées aux personnes définies sur la base des risques.

3.3 Synthèse du contenu

Avec ses 39 articles, la LSIC est volontairement plus courte que la LSI, qui en compte plus de 100, puisqu'elle se borne à définir les principes et à fixer les dispositions touchant à des droits fondamentaux, comme le contrôle de sécurité relatif aux personnes (CSP). L'OSID est par conséquent appelée à régler plus précisément certains éléments, par exemple le management de la sécurité de l'information (MSI), la détermination du besoin de protection des objets à protéger ou la désignation des fonctions nécessitant un CSP. Elle définit en outre les compétences de la CNT et des autres organes de sécurité pour édicter des instructions, arrêter des décisions, conclure des contrats et concevoir des aides à l'exécution concernant la sécurité de l'information et des données. Avec ses 44 articles, l'OSID est elle aussi de taille raisonnable – malgré la reprise d'une partie de l'OPD.

Loi sur la sécurité de l'information et la cybersécurité – LSIC	**Ordonnance sur la sécurité de l'information et des données – OSID**	**Instructions de la CNT sur la sécurité de l'information et des données**
Objectifs d'effet stratégiques, principes et atteintes aux droits fondamentaux 1. Dispositions générales 2. Principes 3. Mesures organisationnelles 4. Mesures techniques 5. Mesures physiques 6. Mesures concernant les personnes 7. Standardisation 8. Organisation de la sécurité 9. Dispositions d'exécution 10. Dispositions finales Délégations au CE en ce qui concerne – la classification – les mesures techniques – les autorités et l'organisation de sécurité – les délais transitoires	Normes sans lien avec les droits fondamentaux et revêtant un caractère tactique : 1. Généralités 2. Principes 3. Mesures organisationnelles 3.1 Management de la sécurité de l'information et des données (MSI) 3.2 Définition des besoins de protection des informations (classification) et des données personnelles 4. Mesures techniques 5. Mesures physiques 6. Mesures concernant les personnes 7. Niveaux de protection 8. Organisation de la sécurité de l'administration cantonale 9. Dispositions d'exécution Délégations à la CNT et à d'autres organes de sécurité	Normes d'exécution à caractère opérationnel : 1. Système MSI 2. Définition des besoins de protection et traitement d'informations (classification) et de données personnelles 3. Procédures et mesures de sécurité 4. Mesures de protection physiques 5. Contrôle de l'identité de personnes et de systèmes et gestion des identités et des accès (IAM) 6. Mesures de sécurité par niveau de protection 7. Outils obligatoires, p. ex. pour l'analyse des besoins de protection, le concept SIPD, etc.

Illustration 4 : Vue d'ensemble de la LSIC, de l'OSID et des consignes SID de la CNT et des autres organes de sécurité

3.4 Organisation de la sécurité du canton et de l'administration cantonale

Conformément à l'article 31 LSIC et à l'article 21, alinéa 2, lettre *a* LAN, l'OSID crée le modèle d'organisation de la sécurité cantonale suivant :

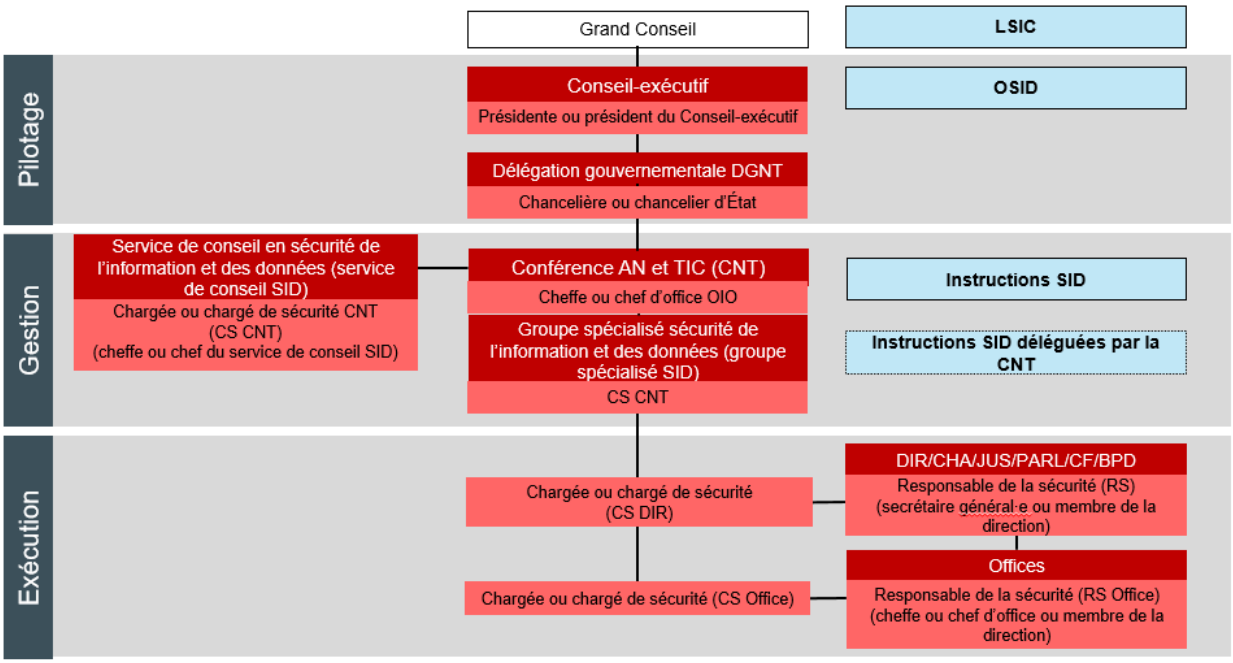


Illustration 5 : Organes chargés de la sécurité de l'administration cantonale

Bien qu'elle confie la responsabilité de la sécurité de l'information et des données à la haute direction, l'OSID prévoit que la CNT édicte des instructions SID lui permettant de déléguer certaines dispositions d'exécution techniques au groupe spécialisé Sécurité de l'information et des données. La Délégation gouvernementale à l'administration numérique et aux TIC (DGNT) peut compléter la CNT par des personnes désignées pour représenter d'autres autorités, comme les communes (art. 18, al. 1, let. *d* OAN).

La garantie de la sécurité incombe aux secrétaires générales et secrétaires généraux des DIR/JUS, à la Chancelière ou au Chancelier d'État, aux cheffes et chefs des Services parlementaires, du Contrôle des finances (CF) ainsi que de l'autorité cantonale de protection des données (à savoir le Bureau pour la protection des données [BPD]), qui, en qualité de responsables de la sécurité (RS), sont tenus de veiller à ce que leur autorité applique les dispositions. Ces personnes peuvent déléguer ce rôle à tout autre membre de la haute direction qui leur est directement subordonné.

L'expertise technique est assurée aux niveaux de la CNT, des DIR/CHA/JUS/PARL/CF, du BPD et des offices par les personnes chargées de la sécurité (CS). La ou le responsable du service de conseil en sécurité de l'information et des données (conseil SID) plus précisément du domaine spécialisé Sécurité de l'OIO exerce également la fonction de chargée ou chargé de sécurité de la CNT et dirige le groupe spécialisé SID.

La CNT est chargée d'édicter les descriptions des rôles ainsi que les tâches, compétences et responsabilités correspondantes.

Il convient de relever que le Bureau du Grand Conseil peut, en ce qui concerne la sécurité de l'information du domaine parlementaire, édicter des dispositions d'exécution qui s'écartent de l'OSID et des instructions adoptées sur sa base (art. 34 LSIC), par exemple en réglant l'organisation et les compétences de ses propres organes de sécurité différemment de l'OSID. Par souci d'harmonisation des dispositions de sécurité, la CNT s'efforcera néanmoins de tenir compte des besoins du Grand Conseil dans ses instructions, afin d'éviter qu'il ne doive se doter de règles dérogatoires.

3.5 Objectifs d'effet

Outre la sécurité de l'information et des données, qui constituent leurs principaux objectifs, la LSIC et l'OSID doivent produire les effets suivants :

a) compréhension des classifications INTERNE, CONFIDENTIEL et SECRET qui soit commune à l'ensemble du canton et à chacun de ses échelons ;
b) réduction du volume d'informations classifiées et amélioration de la protection, c'est-à-dire diminution de la quantité d'informations classifiées au moyen d'une uniformisation et d'une clarification des consignes correspondantes ainsi que de celles régissant la définition du besoin de protection des outils TIC et des données personnelles ;

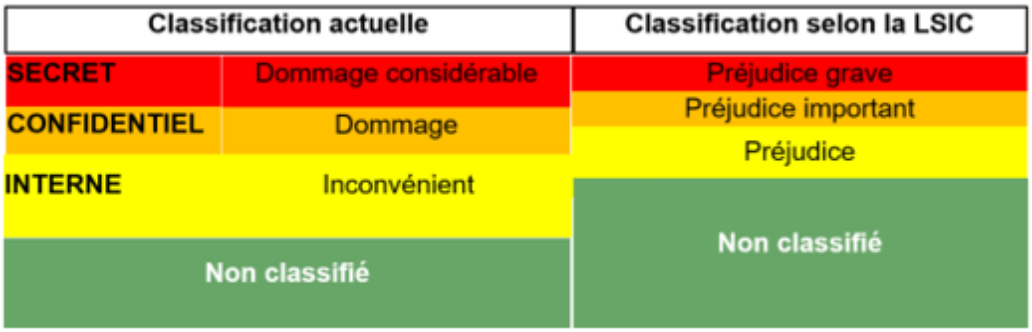


Illustration 6 : Diminution de la quantité d'informations classifiées selon la LSIC

c) réduction des coûts des mesures de sécurité au moyen d'une suppression de celles qui sont inutiles, c'est-à-dire en diminuant la quantité d'informations, de données personnelles et d'outils TIC nécessitant une protection particulière grâce à une définition des besoins de protection adaptée aux risques : « une place pour chaque chose et chaque chose à sa place » ;
d) dispositions cohérentes et uniformes, réparties dans l'OSID, les instructions d'exécution et les aides à l'exécution, concernant la gestion par les autorités bernoises des objets à protéger dont le besoin de protection est défini ;
e) prise de conscience générale de l'importance de la sécurité de l'information et des données de la part du personnel, et en particulier des cadres (sensibilisation) ;
f) existence d'outils permettant aux cadres d'identifier les faiblesses que leur organisation, leurs outils TIC et leurs collaboratrices et collaborateurs représentent en matière de sécurité de l'information et des données ;
g) organisation de la sécurité dotée de responsabilités, tâches et compétences clairement définies, conformément à la structure déjà mise en place en vertu de la LAN.

4. Forme de l'acte législatif

Tant la LSIC que la LCPD délèguent au Conseil-exécutif la compétence d'édicter les dispositions d'exécution relatives à la sécurité de l'information et des données, raison pour laquelle l'OSID est édictée sous la forme d'une ordonnance.

5. Droit comparé

5.1 Confédération

Pour garantir son équivalence avec les réglementations fédérales et permettre au canton de rester reconnu, sans aucune réserve, comme un partenaire doté d'une sécurité moderne et efficace de l'information et des données, l'OSID s'inspire également de l'OSI de la Confédération. Elle est cependant délibérément moins volumineuse et complexe qu'elle, de sorte à demeurer compréhensible et applicable à tous les échelons du canton.

5.2 Cantons

L'examen des législations des autres cantons (en octobre 2025) 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 à la LSIC. Au contraire, certains prennent appui sur la loi bernoise, comme le canton d'Argovie, qui a élaboré une loi sur la sécurité de l'information reprenant largement la structure de la LSIC.

De même, aucun autre canton ne dispose d'une loi sur la protection des données qui renvoie, pour ce qui concerne la sécurité des données, aux mesures de protection nécessaires à la sécurité de l'information.

En proposant ce modèle simplifié, le canton de Berne crée des bases innovantes, axées sur les effets et viables à long terme pour sa sécurité de l'information et des données.

6. Mise en œuvre et évaluation

L'OSID entrera en vigueur à la même date que la LSIC, soit le 1er novembre 2026.
Son exécution sera évaluée selon les processus d'amélioration continue qui seront élaborés dans le cadre de la mise en œuvre et qui constitueront un élément central du système de management de la sécurité de l'information (SMSI) prévu dans l'OSID.

7. Commentaire des articles

7.1 Dispositions générales

Article 1 – Objet

La présente ordonnance repose à la fois sur la LSIC et sur la LCPD. L'OSID règle donc aussi bien la sécurité de l'information que celle des données.

Article 2 – Champ d'application

Alinéa 1 :

Les « autorités cantonales » sont énumérées à l'article 3, lettre *h*. Elles sont tenues de garantir la sécurité des objets à protéger tant du canton que de la Confédération conformément aux règles de l'OSID. En sont exclues les organisations partiellement autonomes visées à l'article 3, alinéa 1 de

l'ordonnance du 27 novembre 2002 sur l'organisation et les tâches de la Direction de l'instruction publique et de la culture (ordonnance d'organisation INC [OO INC][23], voir commentaire de l'art. 3, lit. *h* OSID).

Alinéa 2 :

L'OSID ne s'applique aux autres autorités cantonales que si elles travaillent avec des objets à protéger du canton ou de la Confédération. Par « autres autorités cantonales », on entend par exemple les communes municipales, les communes bourgeoises et les paroisses ainsi que les autres collectivités de droit communal au sens du titre 7 de la Constitution cantonale (ConstC), les Églises nationales au sens du titre 8.1 ConstC et les autres organisations chargées de tâches publiques au sens de l'article 95 ConstC. Les dispositions de l'OSID ne sont donc pas valables, par exemple, pour les informations et applications auxquelles les communes accèdent via BE-Login et AGOV.

Le champ d'application de l'OSID peut être schématisé comme suit :

Champ d'application	**Objets à protéger**	**Autorités canton.**	**Autres autorités**
Sécurité de l'information	Informations / outils TIC du canton ou de la Confédération	OSID Toutes les prescriptions	• OSID - sections 1 et 2 • Mesures de protection prescrites par la Confédération ou le canton (art. 22 OSID) • Mesures de protection supplémentaires adaptées aux risques • Protection de base BE recommandée
	Informations / outils TIC d'autres autorités	OSID Toutes les prescriptions	• OSID non applicable • Protection de base BE recommandée • Mesures de protection supplémentaires adaptées aux risques prises sous leur propre responsabilité
Sécurité des données	Données personnelles	OSID Toutes les prescriptions	• OSID - sections 1 et 2 • Analyse des besoins de protection ou concept SIPD basé sur les risques identifiés et les recommandations de l'autorité de protection des données (art. 8 OSID). • Protection de base BE recommandée

Illustration 7 : Champ d'application de l'OSID

Article 3 – Définitions

Seule la lettre *h* « autorités cantonales » appelle un commentaire.

Les écoles et les institutions de formation cantonales sont des unités administratives partiellement autonomes. Leur organisation, leurs tâches et leurs compétences sont déterminées par la législation (art. 3, al. 1 OO INC). À l'instar des hautes écoles, elles entrent donc dans la définition des « autres organisations chargées de tâches publiques » visées à l'article 95, alinéa 1, lettre *a* ConstC, et sont par conséquent considérées comme des « autres autorités » au sens de l'article 2, alinéa 2 OSID.

[23] OO INC, RSB 152.221.181

7.2 Principes de la sécurité de l'information et des données

Article 4 – Responsabilité des organes de direction

Alinéa 1 :

La haute direction d'une autorité, c'est-à-dire également d'une organisation indépendante ou d'une collectivité accomplissant des tâches de droit public, par exemple, assume une responsabilité particulière dans la garantie de la sécurité de l'information et des données (concernant la haute direction dans l'administration cantonale, voir le commentaire de l'art. 19, al. 1 OSID « Risques résiduels et menaces existantes »).

Lettre *a* : veille à la sécurité de l'information et des données.

La haute direction doit garantir que la sécurité de l'information et des données relevant de son domaine de compétence est conforme à l'évolution technique ; elle doit donc l'organiser et en assurer la mise en œuvre et le contrôle. Elle est tenue, de manière générale, de régler les aspects suivants soit dans des directives de sécurité soit dans des décisions relatives aux risques arrêtées au cas par cas :

a) Les directives de sécurité dictent les objectifs de sécurité de l'information et des données, autrement dit la situation à atteindre. Elles présupposent la réalisation d'une analyse coût-utilité visant à définir le degré de sécurité que l'autorité veut ou doit obtenir et ce que cela peut lui coûter ou lui coûtera.

b) La haute direction doit également déterminer la manière dont les organisations qui lui sont subordonnées doivent gérer les risques, ceux qu'elles sont en droit d'accepter seules et ceux devant faire l'objet d'un rapport à la direction (acceptation des risques). Si la plupart des risques liés à la sécurité de l'information et des données peuvent être traités et assumés au niveau opérationnel (p. ex. office ou unité subordonnée), d'autres revêtent une importance stratégique.

c) Il y a toujours des personnes qui manquent de rigueur et traitent certaines informations, données personnelles ou outils TIC avec négligence ou en n'appliquant pas les règles en vigueur. Bien que ces manquements soient souvent sans conséquence pour leurs auteurs, la haute direction est tenue de veiller à l'application stricte des dispositions ainsi que d'infliger des sanctions disciplinaires et d'engager des procédures pénales si nécessaire.

Lettre *b* : accepte formellement les risques qui subsistent.

En pratique, l'utilisation d'objets à protéger n'est jamais sans risque. Vu que la sécurité absolue n'existe pas, qu'elle est irréalisable ou que son coût serait beaucoup trop élevé, il subsiste toujours des risques malgré les mesures de protection mises en œuvre, risques dits résiduels, que l'autorité compétente doit accepter sciemment et expressément. Cette acceptation « formelle » est importante, car elle prouve que la décision a été prise en connaissance de cause à l'issue d'une analyse des risques et d'un processus décisionnel. Dans l'intérêt de l'accomplissement de ses tâches, l'autorité est ainsi prête à assumer le fait qu'un risque résiduel pourrait se concrétiser.

L'acceptation du risque incombe à l'autorité compétente pour la tâche publique concernée. Pour les outils TIC du canton, elle est détaillée à l'article 32 LAN, qui dispose que l'OIO répond de l'acceptation des risques résiduels dans le domaine des prestations TIC de base et de ses applications de groupe. Les différentes autorités (Directions, offices, autorités judiciaires, Grand Conseil ou autorités de surveillance) sont responsables de l'acceptation des risques résiduels liés aux applications spécialisées et aux applications de groupe relevant de leur domaine de compétence.

Toutes les autorités répondent en outre de l'acceptation des risques résiduels liés à la manière dont elles utilisent les outils TIC mis à leur disposition par d'autres autorités (p. ex. si un office envoie par courriel des informations à protéger sans les crypter).

Alinéa 2 :

Les responsables hiérarchiques de chaque échelon sont chargés de s'assurer que leur personnel ou leurs mandataires aient une formation initiale et continue adaptée à leur fonction et à leur travail sur le terrain, et à ce qu'ils respectent les prescriptions. Cette responsabilité s'étend aussi à la sécurité de l'information et des données. Les collaboratrices et collaborateurs tout comme les mandataires doivent être en mesure d'identifier eux-mêmes les dangers et les menaces, d'y réagir correctement et de transmettre les signalements de sécurité qui s'imposent. Les autorités veillent à ce que la formation soit assurée, par exemple à l'entrée en fonction ou via des campagnes de sensibilisation régulières.

En collaboration avec l'autorité cantonale de protection des données, le service de conseil SID met à la disposition des autorités des ressources générales (p. ex. le cours en ligne BE-Secure) et organise des campagnes de sensibilisation à l'intention des autorités cantonales, par exemple des simulations d'hameçonnage. Le cours BE-Secure proposé actuellement prend deux heures au plus, s'adresse à tout le personnel et est également ouvert à des personnes ne faisant pas partie des autorités cantonales. Les campagnes de sensibilisation se poursuivront grâce aux ressources dédiées du domaine Sécurité de l'OIO.

Pour aider les responsables à assumer leurs obligations concernant la formation et son contrôle, le service de conseil SID peut également leur fournir des informations sur la participation aux cours et les résultats obtenus par les collaboratrices et collaborateurs concernés.

Alinéa 3 :

Les responsables hiérarchiques de chaque échelon et le personnel travaillant avec des objets à protéger sont tenus de respecter les codes de conduite établis dans la législation. Pour pouvoir assumer cette responsabilité, les collaboratrices et collaborateurs doivent toutefois avoir reçu les instructions nécessaires, avoir été formés en conséquence et disposer des ressources nécessaires. Par *collaboratrices et collaborateurs*, on entend l'ensemble du personnel et des collaboratrices et collaborateurs externes soumis au pouvoir d'instruction de l'autorité : le personnel désigne les employées et employés de l'autorité au sens du droit du personnel cantonal ou communal, tandis que les collaboratrices et collaborateurs externes sont les personnes appelées à travailler pour l'autorité sur la base d'un contrat de location de services.

Ne sont pas considérés comme des collaboratrices et collaborateurs les particuliers travaillant à titre d'indépendant ou le personnel d'entreprises agissant auprès de l'autorité comme consultant dans le cadre d'un contrat de droit privé au sens du code des obligations[24] ou comme fournisseur de biens ou services (p. ex. développement d'un logiciel, création d'un réseau, construction d'une salle de serveurs ou direction d'un projet). Ces personnes doivent être gérées comme des tiers mandatés conformément aux prescriptions de l'article 17. Cela vaut aussi pour les bénévoles, notamment celles et ceux qui s'engagent dans des paroisses.

[24] CO, RS 220

Alinéa 4 :

La haute direction reste dans tous les cas responsable de la garantie de la sécurité de l'information et des données, y compris pour les unités qui lui sont subordonnées et les tiers mandatés. En particulier lorsqu'elle fait appel à des prestataires privés, il lui appartient de les sélectionner, de les informer et de les surveiller soigneusement et, le cas échéant, de s'en séparer ou de les sanctionner.

Article 5 – Mesures de prévention

L'article 10, alinéa 1 LCPD dispose que toute personne doit garantir une sécurité adéquate aux données qu'elle traite, tandis que l'ordonnance sur la protection des données en vigueur régit les exigences relatives aux mesures de protection techniques, organisationnelles, physiques et liées au personnel requises pour la protection de base (art. 4 ss OPD). L'OSID reprend ces dispositions et les actualise à la lumière du droit fédéral. Elle s'appuie ainsi sur un fondement général et abstrait pour formuler les éléments de la protection globale tant des informations que des données personnelles, à savoir la protection de base.

Cet article définit les objectifs d'effet à atteindre pour chaque objet à protéger, qu'il soit numérique ou analogique, dans les quatre dimensions de la sécurité de l'information et des données. Il est formulé de manière générale, car les mesures de protection concrètes propres à chaque niveau de protection sont définies par la CNT dans l'instruction sur la protection de base en matière de sécurité de l'information et des données du canton de Berne (Protection de base BE). Toute mesure de protection supplémentaire prise pour satisfaire à des exigences de sécurité accrues doit être décrite dans le concept de sécurité de l'information et de protection des données (concept SIPD). Les mesures de protection doivent toujours être définies en fonction du risque qui pèse sur l'objet à protéger. En d'autres termes, elles doivent être adaptées aux risques.

Lettre *a* : confidentialité

Le contrôle d'accès aux données est une mission essentielle des autorités pour garantir la sécurité de l'information et des données : seuls les membres des autorités doivent pouvoir y accéder, et uniquement pour accomplir leurs tâches légales. Outre l'accès lui-même, il convient de définir et de contrôler son étendue et les droits afférents.

Le contrôle d'accès aux locaux et aux installations utilisés pour traiter des données consiste par exemple à désigner les personnes autorisées à y accéder. Les « installations » englobent aussi les appareils de traitement mobiles. Utilisé dans une acception très large, ce terme recouvre tous les appareils utilisés pour traiter des données personnelles, des centres de calcul fixes équipés de salles de serveurs aux ordinateurs, en passant par les téléphones mobiles et les tablettes. Différentes mesures peuvent être mises en place dans ce cadre, par exemple les systèmes d'accès individuel avec contrôle d'identité biométrique ou l'identification sécurisée lors de la connexion à son propre PC ou ordinateur portable.

S'agissant du contrôle d'identité, les autorités doivent également s'assurer que seules les personnes autorisées puissent avoir accès à des applications contenant des informations non publiques ou des données personnelles. Parmi les mesures simples à mettre en place figurent le contrôle et la mise à jour réguliers des droits d'accès, le blocage automatique des comptes d'utilisateur qui n'ont pas été utilisés depuis plus d'un an ou l'installation d'un logiciel contre les maliciels ou les logiciels espions.

Lettre *b* : disponibilité et intégrité

Le contrôle des supports de données vise à garantir la disponibilité et l'intégrité des informations et des données personnelles, par exemple au moyen d'un système de cryptage ou d'autorisations d'accès granulaires aux applications et aux systèmes d'exploitation. Les autorités doivent en outre prendre des mesures appropriées pour protéger les données lors de leur communication ou lors du transport de supports de données (contrôle du transport). Là aussi, il est possible de recourir à l'identification sécurisée des personnes ou au cryptage des informations ou des données personnelles (ch. 1).

L'un des moyens permettant de garantir la restauration rapide de la disponibilité et de l'accessibilité des données personnelles et des informations après une panne est d'installer un système de sauvegarde de sécurité (ou *backup*) prévoyant la réplication des données sur des supports ou dans des centres de calcul (ch. 2).

La stabilité et la capacité de traitement des outils TIC utilisés doivent être garanties à long terme (ch. 3), en veillant à ce que toutes les fonctions du système de traitement de données informatisé soient disponibles (disponibilité), que les dysfonctionnements soient signalés (fiabilité) et que les informations et données personnelles stockées ne puissent pas être endommagées par des dysfonctionnements du système (intégrité de l'information et des données).

Enfin, il convient de garantir la sécurité des systèmes (ch. 4), en effectuant systématiquement les mises à jour de sécurité des systèmes d'exploitation et des applications logicielles et en corrigeant les vulnérabilités identifiées.

Lettre *c* : traçabilité

Pour des raisons économiques, la traçabilité systématique des modifications apportées aux informations ne doit être assurée qu'à partir de la classification « INTERNE ». S'agissant des données personnelles, elle doit être garantie indépendamment de leur besoin de protection.

Le contrôle de la saisie (ch. 1) impose de pouvoir vérifier a posteriori les informations ou les données personnelles introduites ou modifiées dans des systèmes informatisés, le moment où l'opération a eu lieu et l'identité des personnes qui s'en sont chargées. L'une des mesures possibles à cet effet est la journalisation visée à l'article 6 ci-après, mais il en existe d'autres, comme

a) la limitation des droits à quelques rares personnes,
b) le contrôle physique de l'accès à l'application,
c) la limitation de la disponibilité de l'application à une durée très courte,
d) l'enregistrement de l'heure exacte de chaque accès, ou
e) une combinaison de ces différentes mesures.

Le contrôle de la communication (ch. 2) doit notamment permettre d'identifier les destinataires des données : selon les cas, il peut suffire à cet égard d'indiquer l'autorité à laquelle les données sont destinées, sans forcément préciser qui agit en son nom. En cas de besoin, des enregistrements doivent permettre de retrouver les outils utilisés, les données personnelles transmises et les destinataires concernés.

Les mesures de détection et de résolution des incidents de sécurité (ch. 3) sont réactives et doivent être définies comme telles dans des plans de prévention.

Article 6 – Journalisation du traitement informatisé de données personnelles

Alinéa 1 :

L'obligation de journalisation fait partie des mesures supplémentaires de garantie de la sécurité des données prévues dans l'hypothèse où les mesures préventives visées à l'article 5 ne suffiraient pas. Cet article précise donc les mesures de protection destinées à garantir la traçabilité lors du traitement informatisé de données personnelles, c'est-à-dire essentiellement lorsqu'une personne dispose de droits extrêmement étendus ne pouvant être limités en amont aux seules données dont elle a besoin pour s'acquitter de ses tâches. Le traitement « informatisé » correspond au traitement « automatisé » figurant dans le droit bernois en vigueur (art. 6, al. 1 OPD) et dans le droit fédéral (art. 4, al. 1 et 2 de l'ordonnance du 31 août 2022 sur la protection des données [ordonnance sur la protection des données, OPDo])[25] et consiste donc en un traitement de données généralement effectué sans intervention ni vérification humaine.

La journalisation n'a pas pour principal objectif de surveiller les utilisatrices et utilisateurs mais bien plutôt

a) de permettre aux autorités confrontées à des risques particuliers de contrôler a posteriori le traitement de données personnelles, afin de déterminer si certaines d'entre elles ont été perdues, effacées, détruites, modifiées ou divulguées,
b) de fournir des indications sur l'adéquation et, partant, la conformité légale du traitement des données personnelles.

Selon l'alinéa 1, les autorités journalisent au moins l'enregistrement, la modification, l'effacement et la destruction des données. En journalisant le traitement informatisé des données personnelles, elles garantissent sa traçabilité et s'acquittent ainsi aussi de leurs obligations au sens de l'article 5, lettre *c*.

Alinéa 2 :

Si des autorités ou des tiers mandatés procèdent au traitement informatisé de données personnelles sensibles ou à un profilage à risque élevé alors que, malgré les mesures de prévention visées à l'article 5, la sécurité des données n'est pas suffisamment garantie, ils journalisent en outre l'accès aux données personnelles ainsi que leur lecture et leur communication. Prenons l'exemple de membres du corps de police qui disposent sur leur téléphone mobile d'un accès étendu aux bases de données de la police : cet accès ne peut pas être limité en amont, car il est impossible de prévoir qui les policières et policiers vont rencontrer dans le cadre de l'accomplissement de leurs tâches. Le cas échéant, il est indispensable de consigner la lecture des données personnelles pour pouvoir retracer et sanctionner toute consultation effectuée hors du cadre du service.

Cette disposition s'inspire de l'article 4, alinéa 2 de l'OPDo de la Confédération et précise que la lecture et la communication de données doivent être consignées uniquement lorsque l'analyse des besoins de protection révèle que les mesures préventives sont insuffisantes. Il satisfait ainsi aussi aux exigences du droit européen concernant la journalisation définies à l'article 25 de la directive (UE) 2016/680 en lien avec la poursuite pénale et l'exécution des peines, puisque les données relevant du champ d'application de la directive sont en principe sensibles.

Le procès-verbal de journalisation devrait contenir :

a) l'identité du système ou de la personne traitant des données qui accède à des informations ou données personnelles via le système,
b) la nature du traitement,

[25] OPDo, RS 235.11

c) la date et l'heure du traitement,
d) le cas échéant, l'identité de la personne à laquelle les données personnelles sont destinées.

En cas de suspicion d'utilisation abusive des informations ou des données personnelles, les autorités doivent pouvoir les mettre rapidement à l'abri, à l'intention de l'autorité de poursuite pénale.

Alinéa 3 :

Les procès-verbaux de journalisation sont conservés au moins six mois. Faute de ressources suffisantes, le législateur renonce, contrairement à la Confédération, à imposer de manière générale un délai d'une année, préférant définir un délai minimal à prolonger en fonction du risque identifié pour l'application concernée. Les procès-verbaux doivent être tenus et conservés de manière à pouvoir retracer un événement durant les six mois suivant sa survenance.

Ceux portant sur des informations classifiées « CONFIDENTIEL » et « SECRET » ainsi que sur des données personnelles sensibles (nouvelle terminologie selon la LCPD remplaçant données personnelles particulièrement dignes de protection) et des données personnelles dont la divulgation pourrait représenter une menace pour la vie et l'intégrité corporelle des personnes concernées doivent être conservés plus longtemps, car sinon, les chances d'établir la preuve de leur utilisation abusive et, partant, d'engager réellement une poursuite pénale et d'obtenir un effet dissuasif efficace seraient trop faibles.

Les procès-verbaux particulièrement susceptibles d'être volés, détruits, effacés, manipulés ou cryptés lors d'un incident de sécurité doivent être conservés à l'extérieur du système dans lequel les données personnelles sont traitées. C'est notamment le cas pour les procès-verbaux de journalisation des automates de surveillance des feux rouges, de la vitesse et des interdistances qui peuvent être détruits sur place ou volés, et doivent donc être envoyés ailleurs.

L'accès aux procès-verbaux est réservé aux services chargés de la surveillance des prescriptions relatives à la protection des données ou d'autres tâches légales. Les procès-verbaux ne peuvent utilisés qu'à ces fins. Comme cette règle figure déjà dans la disposition générale de l'article 6 LCPD définissant la finalité, il est inutile de la reprendre expressément dans l'ordonnance.

Article 7 – Signalement des incidents de sécurité, des vulnérabilités et des cyberattaques

Afin de protéger la Suisse contre les cybermenaces, l'Office fédéral de la sécurité (OFCS) réalise des analyses techniques pour évaluer et contrer les cyberincidents et les cybermenaces, ainsi que pour identifier et éliminer les vulnérabilités (art. 73*a*, al. 1 LSI). Le principal objectif de l'introduction de l'obligation de signaler au niveau cantonal est de faciliter la détection précoce et la vue d'ensemble des menaces (voir aussi le Message relatif à la modification de la loi sur la sécurité de l'information [Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques] du 2 décembre 2022, ch. 4.1[26]). L'obligation de signaler s'inscrit donc dans le cadre de l'obligation de planification préventive et de réactivité au sens de l'article 7, alinéa a LSIC et fait ainsi partie des mesures de protection préventives visées à l'article 5, lettre *c*, chiffre 3 OSID tant pour protéger les informations que les données personnelles.

Étant donné que les pirates informatiques utilisent souvent des méthodes et des schémas similaires pour plusieurs infrastructures critiques de différents secteurs, cette obligation peut contribuer de manière significative à renforcer la sécurité de l'information et des données en favorisant la détection précoce des méthodes utilisées et l'émission d'alertes appropriées. Elle engendre un grand nombre de signalements, ce qui améliore aussi l'évaluation du risque et la manière de le contrer.

[26] FF 2023 84

En matière de menaces ou d'atteintes à la sécurité de l'information ou des données, les autorités bernoises sont soumises à trois lois, l'une fédérale et les autres cantonales, prévoyant toutes des obligations de signaler spécifiques assorties de buts, de délais et de contenus différents :

a) articles 26 ss LCPD - buts : protéger les personnes concernées et d'autres victimes potentielles, accroître la transparence et améliorer la sécurité des données ; délai : 72 heures à partir de la découverte de la violation de la sécurité de l'information (art. 26, al. 1 LCPD) ;
b) article 7 LSIC - l'obligation de prévenir et de réagir faite aux autorités implique l'obligation de signaler les incidents de sécurité, les vulnérabilités ou les cyberattaques ;
c) articles 73*b* ss LSI - but : protéger les autorités, organisations ou personnes concernées ainsi que d'autres victimes potentielles ; délai : 24 heures à partir de la découverte de la vulnérabilité ou de la cyberattaque (art. 74*e*, al. 1 LSI).

S'agissant de ce dernier point, la Confédération cite en outre expressément, à l'article 74*b* LSI, les nombreuses autorités et organisations assujetties à l'obligation de signaler, parmi lesquelles les autorités cantonales mais aussi les « autorités communales » (alinéa 1, lettre *b*). Renseignements pris auprès de l'OFCS, le terme « autorités communales » englobe toutes les collectivités de droit public au sens du droit cantonal qui accomplissent des tâches régaliennes, c'est-à-dire également les communes municipales, les paroisses et les communes bourgeoises ainsi que les organisations indépendantes assumant pour elles des tâches publiques.

Certes, l'obligation de signaler fixée à l'article 74*a*, alinéa 1 LSI porte uniquement sur les cyberattaques, mais étant donné que le signalement de tous les incidents de sécurité s'inscrit dans le cadre du devoir de planification et de réactivité prescrit à l'article 7, lettre *a* LSIC, il est essentiel à la mesure de sécurité que les autorités bernoises sont tenues d'appliquer en vertu de l'article 5, lettre *c*, chiffre 3 OSID, à savoir la détection et la réparation rapides des conséquences d'incidents de sécurité.

Les trois bases légales sur lesquelles repose l'obligation de signaler instituent au total trois destinataires différents : les autorités bernoises de protection des données, le service cantonal de conseil SID et l'OFCS. La présente disposition permet aux personnes assujetties à l'obligation de signaler de s'acquitter facilement de leur tâche légale en utilisant le même outil TIC pour les trois autorités concernées.

Alinéa 1 :

L'obligation de signaler ne concerne pas tous les incidents liés à la sécurité, mais uniquement ceux qui représentent une menace importante ou ont déjà porté concrètement atteinte à la sécurité de l'information et des données. Les incidents de sécurité, les vulnérabilités ou les cyberattaques doivent notamment être signalés dans les cas suivants :

a) Ils entravent l'accomplissement des tâches des collaboratrices et collaborateurs ou de tiers mandatés.

   L'accomplissement des tâches est réputé entravé au plus tard quand la disponibilité d'informations, de données personnelles ou d'outils TIC est compromise. Cela peut toutefois aussi être le cas au moment où l'on constate que des informations ou des données personnelles ont été falsifiées, anéantissant leur intégrité.

b) Ils menacent la sécurité d'objets à protéger des niveaux de protection 2 et supérieurs, c'est-à-dire :

   1. des informations classifiées CONFIDENTIEL ou SECRET ;

2. des données personnelles sensibles ou dont la divulgation est susceptible de représenter un danger grave pour la sécurité des personnes concernées ;
3. des outils TIC rattachés aux catégories « protection élevée » et « protection très élevée ».

La gravité des conséquences de la violation de leur sécurité peut être telle que la simple mise en péril de ces objets nécessite un signalement, par analogie à l'article 74*d*, lettre *a* LSI relative à la mise en péril du fonctionnement d'une infrastructure critique. Le danger doit être imminent, mais pas inévitable, à l'instar des infractions de mise en danger figurant dans le Code pénal suisse du 21 décembre 1937 (CP)[27].

c) Ils pourraient avoir une portée politique importante :

L'obligation de signaler peut également s'imposer lorsqu'il existe un risque que des incidents de sécurité, des vulnérabilités ou des cyberattaques aient une portée politique importante, sans que les deux critères précités soient remplis. L'importance de la portée politique d'un incident dépend des autorités ou des objets à protéger concernés, mais aussi des circonstances entourant l'incident. Vu la possibilité d'évolution de la portée politique, ce critère est soumis à l'évaluation du service de conseil SID, qui travaille en collaboration avec la ou le RS.

Exemples d'incidents de sécurité devant être signalés :

- Un collaborateur adresse par erreur un important volume de données contenant des informations confidentielles (niveau de protection 2) à une personne externe au lieu de l'envoyer à sa supérieure hiérarchique ;
- les droits d'accès à une application de gestion du personnel ont été mal paramétrés, de sorte que tout le personnel de l'administration, et non pas uniquement celui du service du personnel, peut consulter les dossiers des collaboratrices et collaborateurs ;
- une faille a été détectée dans un logiciel de gestion d'affaires utilisé à large échelle.

Alinéa 2 :

La LSI et la LCPD prévoient des délais de signalement différents, ce que met en exergue cet alinéa.

Alinéa 3 :

Pour autant que l'article 27 LCPD l'y oblige, l'autorité est tenue d'informer la personne concernée par la violation de la sécurité des données en lui communiquant, en des termes simples, au moins les indications énoncées.

Tout signalement de violations de la sécurité de l'information et des données doit en outre comprendre au minimum les indications suivantes, pour autant qu'elles soient évaluables et disponibles (voir aussi l'art. 15 OCyS) :

a) date et heure du constat de l'incident de sécurité, de la vulnérabilité ou de la cyberattaque,
b) date et heure de l'incident de sécurité ou de la cyberattaque,
c) description de l'atteinte à la disponibilité, à l'intégrité, à la confidentialité ou à la traçabilité des informations ou des outils TIC,
d) étendue de l'atteinte à la capacité de fonctionnement de l'autorité,
e) mesures prises et planifiées pour restaurer et garantir la sécurité de l'information à l'avenir.

Si certaines des informations requises font défaut au moment du signalement, elles doivent être complétées dès que de nouveaux éléments sont disponibles.

[27] CP RS 311.0

Alinéa 4 :

Pour pouvoir fonctionner, le système de signalement doit être simple, uniformisé et à bas seuil. Le service de conseil SID fournit donc aux personnes assujetties aux obligations de signalement une plateforme cantonale, disponible sur Internet à l'adresse www.be.ch/isds, leur permettant de s'acquitter de toutes les obligations de signalement auprès des trois destinataires concernés.

Les autorités doivent organiser leur système de signalement de sorte qu'il fonctionne parfaitement, en définissant en amont les tâches, les compétences, les responsabilités et les processus à l'interne, mais aussi et surtout à l'égard de leurs tiers mandatés. Pour ce faire, chaque autorité doit instituer un guichet unique interne. Dans une Direction cantonale ou une ville, le plus judicieux est de désigner un guichet par office, dans une grande commune un guichet par service et dans une autorité de moindre envergure, de désigner comme tel la personne qui la dirige, par exemple. Chacun de ces guichets de signalement internes communique ensuite les cas via la plateforme cantonale.

Chaque autorité doit en particulier définir les éléments suivants en amont et à l'égard de leurs tiers mandatés :

a) le guichet unique de signalement auquel doit être signalé tout incident de sécurité, toute vulnérabilité ou toute cyberattaque,
b) la manière de les signaler,
c) comment les gérer,
d) qui peut ordonner des mesures d'urgence.

Étant donné que l'obligation de signaler au sens de l'article 74*b*, alinéa 1 LSI s'adresse aussi à différents fournisseurs d'outils TIC, ces derniers doivent également procéder spontanément aux signalements via la plateforme visée à l'alinéa 4 et auprès de l'autorité qui les a mandatés aux termes de leur contrat. On accepte ainsi l'éventualité que le guichet unique de l'autorité mandante signale le même incident.

Article 8 – Analyse des besoins de protection et concept SIPD d'autres autorités

Les autorités du canton de Berne doivent toutes procéder à une analyse au sens de l'article 18 LCPD pour évaluer les risques liés aux données personnelles qu'elles utilisent. Le cas échéant, elles doivent prendre des mesures de protection conformes à l'analyse d'impact relative à la protection des données personnelles visée à l'article 19 LCPD pour limiter les risques particuliers et ainsi garantir le niveau de sécurité des données requis. La marche à suivre pour la protection des informations est la même, sauf que les étapes correspondantes s'appellent « analyse des besoins de protection » et « concept SIPD ». Par souci de simplicité et de clarté, les articles 13 et 16 OSID emploient la même terminologie dans les deux cas applicables aux autorités cantonales, à savoir « analyse des besoins de protection » et « concept SIPD ».

Le présent article précise qu'en ce qui concerne les risques liés aux données personnelles, la situation des autres autorités au sens de l'article 2, alinéa 2 OSID est différente de celle des autorités cantonales. Ainsi, la plupart des collectivités de droit communal traitent nettement moins de données personnelles que les autorités cantonales, qui ont par exemple accès, via la plateforme des systèmes des registres communaux (GERES), aux données personnelles des près de 1,1 million de personnes inscrites dans le canton. En outre, les collectivités de droit communal ont généralement des connaissances techniques et des ressources en matière de sécurité des données plus limitées que les autorités cantonales.

C’est la raison pour laquelle, tout en exigeant aussi des autres autorités qu’elles présentent, en vue du contrôle préalable (art. 9 OSID), une analyse des besoins de protection (et, si nécessaire, un concept SIPD) attestant du respect de leurs obligations en vertu du droit sur la protection des données, l’OSID prévoit que l’autorité cantonale de protection des données publie des recommandations et modèles de document spécifiquement adaptés aux risques des autres autorités (art. 9, al. 4 OSID).

Article 9 – Contrôle préalable

Il découle de l’article 3, alinéa 1, lettre *b* LSIC en relation avec l’article 10, alinéa 2 LCPD que les mesures de protection pour la sécurité de l’information sont les mêmes que pour la sécurité des données, comme l’illustrent les niveaux de protection figurant à l’annexe 1.

Le contrôle préalable visé à l’article 20 LCPD est l’instrument dont disposent les autorités de protection des données pour vérifier si le projet de traitement de données personnelles au moyen d’un outil TIC garantit la sécurité de l’information selon l’article 10 LCPD, la LSIC ou l’OSID et est ainsi conforme au droit sur la protection des données. Le résultat du contrôle répond à une question de fait qu’il convient de clarifier avant de pouvoir confirmer que la protection des données respecte les prescriptions légales. Le contrôle doit par essence avoir lieu avant le traitement des données ou la mise en service de l’outil TIC.

L’autorité de protection des données s’en sert toutefois aussi pour vérifier le respect d’autres conditions légales applicables au traitement licite de données personnelles et principalement si :

1. le traitement des données personnelles est prévu par la législation ou sert à accomplir une tâche légale (art. 4, al. 1 LCPD) ;
2. le traitement des données personnelles sensibles est prévu par une loi, indispensable à l’accomplissement d’une tâche légale ou autorisé par la personne concernée (art. 4, al. 2 LCPD) ;
3. les données personnelles et la nature du traitement sont dans les deux cas appropriées et nécessaires à l’accomplissement de la tâche légale tout en étant acceptables pour la personne concernée (selon le principe de proportionnalité, art. 7 LCPD).

Étant donné qu’il consiste essentiellement à vérifier la sécurité des données, le contrôle préalable et les critères déterminant sa nécessité sont réglés dans l’OSID.

Alinéa 1 :

Si l’autorité est tenue de soumettre un projet de traitement de données à l’autorité de protection des données pour contrôle préalable, elle doit aussi lui soumettre les modifications importantes concernant ce traitement (art. 20, al. 2 LCPD). Ces modifications doivent être soumises à l’autorité de protection des données pour contrôle préalable dans les conditions applicables jusqu’ici (voir encore art. 7, al. 3 OPD).

C’est le cas lorsque les moyens ou la finalité du traitement des données changent considérablement. La finalité est un élément fondamental de la législation sur la protection des données (art. 6 LCPD). Quant aux moyens employés pour le traitement de données, ils déterminent généralement l’ampleur de l’atteinte. S’ils changent considérablement, un contrôle préalable s’impose donc aussi. S’ils demeurent identiques, mais que la finalité du traitement des données change, un nouveau contrôle préalable doit être effectué afin de vérifier que le but visé repose toujours sur une base légale suffisante (art. 6, al. 2, lit. *b* LCPD).

Un contrôle préalable est par ailleurs indispensable lorsque la modification est si importante qu’elle remplit à elle seule les conditions d’un contrôle préalable, par exemple si la centrale des amendes

d'ordre s'équipe d'un système en réseau de contrôle de la vitesse et des feux rouges. Toute modification de système de cette nature doit faire l'objet d'un contrôle préalable.

Alinéa 2 :

Comme jusqu'à présent, la modification n'est en principe pas réputée importante lorsque le traitement des données s'étend sans sortir du cadre fixé, car il est alors admis que le degré de l'atteinte aux droits individuels reste inchangé. Ce cadre est défini à l'alinéa 3, lettre *b*.

Alinéa 3 :

En vertu de l'article 20 LCPD, l'autorité doit soumettre un traitement de données au contrôle préalable de l'autorité de protection des données s'il existe un risque élevé pour la personne concernée. Ce risque doit de manière générale être évalué au cas par cas. Dans les deux cas mentionnés dans cet alinéa, on peut cependant partir du principe qu'il n'existe pas de risque élevé pour la personne concernée et qu'il est possible de renoncer à un contrôle préalable.

Ainsi, il est prévu de maintenir la dérogation à l'obligation de contrôle préalable visée à l'article 9, alinéa 1, lettre *a* OPD en vigueur, c'est-à-dire en présence d'une certification satisfaisant aux conditions fixées dans la loi fédérale du 25 septembre 2020 sur la protection des données (loi sur la protection des données, LPD)[28]. Cette disposition doit toutefois être modifiée : dans le cadre de la révision qui conduira à l'OCPD, les conditions de dérogation seront adaptées à la teneur de la LPD révisée, selon laquelle des systèmes, des produits ou, ce qui est nouveau, des services peuvent être certifiés. En outre, cette dérogation ne s'applique désormais plus uniquement aux communes et aux autres collectivités de droit communal. Tout laissant par ailleurs supposer que dans tous les cas le risque est faible pour la personne concernée lorsque des outils TIC sont certifiés conformément à l'article 13 LPD.

Alinéa 4 :

N'appelle aucun commentaire.

Article 10 – Exploitation d'outils TIC

Alinéa 1 :

Les autorités sont responsables de la sécurité des outils TIC qu'elles emploient pour traiter des informations et des données dans le cadre de leur travail. Elles en surveillent donc l'utilisation et vérifient régulièrement qu'ils sont sûrs. La fréquence des contrôles dépend des résultats de l'évaluation des risques effectuée pour chaque application. La surveillance porte sur les aspects purement techniques de la sécurité et porte uniquement sur le comportement du personnel en lien avec la sécurité.

Les autorités peuvent confier ces tâches à des tiers indépendants et qualifiés, comme un fournisseur privé de services de sécurité (*Managed Security Service Provider*, MSSP) ou l'exploitant d'un programme de primes aux bogues (voir art. 40 OSID). Dans ce contexte, elles doivent veiller à ne pas mandater des tiers qui sont en concurrence directe avec les fournisseurs de prestations contrôlés, afin d'éviter que leurs secrets d'affaires ne tombent entre les mains de concurrents. Les mandataires doivent en outre disposer des compétences techniques nécessaires et, en tant qu'auxiliaires des autorités, être informés du secret de fonction et des sanctions pénales prévues à cet égard en vertu de l'article 320 CP.

[28] LPD, RS 235.1

Alinéa 2 :

N’appelle aucun commentaire.

Article 11 – Autorisations restrictives

Alinéa 1 :

Cette disposition rappelle un principe fondamental de la sécurité de l’information et des données, à savoir qu’il est primordial d’accorder aux collaboratrices et collaborateurs ainsi qu’aux mandataires uniquement les droits d’accès dont ils ont effectivement besoin pour accomplir leurs tâches. En les empêchant de traiter sans motif des informations ou des données personnelles d’un autre domaine, on réduit considérablement les risques d’utilisation abusive. Il arrive qu’au terme de leur contrat de travail, de leur mandat ou d’une mission particulière, les collaboratrices et collaborateurs 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 licites, peuvent alors être utilisés contre les intérêts des autorités. Il faut donc veiller à les leur retirer à la fin de leur engagement, de leur mandat ou de leur mission.

Alinéa 2 :

S’il y a lieu de croire que la sécurité de l’information ou des données est compromise, les autorisations doivent immédiatement être bloquées ou retirées. L’objectif principal de ces deux mesures est de réduire le risque d’un acte interne.

Alinéa 3 :

Le contrôle des quelque 10 000 droits d’accès à GERES effectué chaque année par l’OIO auprès des autorités, cantonales et autres, illustre clairement le fait que, malgré les procédures bien définies régissant l’engagement et le départ de membres du personnel, il arrive régulièrement que des droits d’accès subsistent inutilement pendant longtemps. Il est donc essentiel de les vérifier périodiquement en tenant compte du besoin de protection des outils TIC.

Article 12 – Collaboration entre les autorités

Alinéa 1 :

N’appelle aucun commentaire.

Alinéa 2 :

Cet alinéa autorise les services compétents à se communiquer mutuellement des données personnelles dans le but d’accomplir leurs tâches et d’assurer leur propre protection. L’échange doit cependant servir uniquement le but légal qu’est la garantie de la sécurité de l’information et des données. C’est notamment le cas lors de la transmission d’informations indiquant l’identité des victimes d’un incident de sécurité, la nature de l’atteinte et si ces personnes ont déjà été contactées ou informées.

7.3 Mesures de protection des autorités cantonales

7.3.1 Procédure de sécurité applicable aux outils TIC

Cette section repose aussi bien sur les articles 11 et suivants LSIC (Analyse des besoins de protection et concept SIPD) que sur les articles 18 et suivants LCPD (Analyse des risques et analyse d'impact relative à la protection des données personnelles). Bien que ces dispositions ne s'appliquent qu'aux autorités cantonales, les autres autorités sont elles aussi tenues, en vertu des articles 18 à 20 LCPD, d'analyser les risques et l'impact de la protection des données. Dans ce contexte, elles réalisent leur analyse des besoins de protection et établissent leur concept SIPD en tenant compte de leurs propres risques et des recommandations (art. 8 OSID) ou des consignes (art. 9, al. 4 OSID) de leur autorité de protection des données.

Article 13 – Analyse des besoins de protection

Alinéa 1 :

L'évaluation des risques par les autorités cantonales est indispensable pour garantir l'efficacité de la gestion des risques et, partant, l'adéquation et la rentabilité de la sécurité de l'information et des données. Les autorités cantonales sont tenues d'évaluer le besoin de protection des outils TIC ainsi que des informations et des données personnelles qui y sont traitées.

Alinéa 2 :

Mettre un outil TIC en service en l'absence d'une analyse des besoins de protection reviendrait pour les responsables à accepter sciemment de compromettre la sécurité des informations ou des données personnelles. Cela peut être assimilé à une violation intentionnelle du secret de fonction ou de la personnalité des personnes concernées et donc entraîner des conséquences non seulement pénales et civiles, mais aussi disciplinaires. Si l'outil TIC considéré est soumis à l'obligation de contrôle préalable, la violation peut en outre conduire l'autorité de protection des données à ordonner par décision la modification ou la mise hors service de l'outil concerné, comme le prévoit l'article 48 LCPD.

Article 14 – Protection de base

Les autorités cantonales sont tenues de garantir pour tous les objets à protéger la protection de base BE définie par la CNT.

Les autres autorités veillent à la sécurité de l'information et des données en prenant les mesures préventives et adaptées aux risques visées aux articles 5 et 6 OSID ; il leur est recommandé d'assurer la protection de base BE. Si elles utilisent des objets à protéger du canton ou de la Confédération, elles doivent appliquer les mesures de protection figurant dans l'instruction, la décision ou le contrat correspondant (art. 22 OSID).

La protection de base BE est une directive d'exécution visant à soulager les autorités concernées : en la mettant en œuvre, documentation à l'appui, l'autorité et ses collaboratrices et collaborateurs s'acquittent de leurs obligations (minimales) légales. Les autorités et les tiers mandatés fournissant des prestations aux autorités cantonales doivent pouvoir prouver aux autorités de surveillance et aux mandants qu'ils respectent les exigences liées à la protection de base.

Le champ d'application de la protection de base BE peut être schématisé comme suit :

Champ d'application	Objets à protéger	Autorités canton.	Autres autorités
Sécurité de l'information	Informations / outils TIC du canton ou de la Confédération	Protection de base BE	• Mesures de protection prescrites par la Confédération ou le canton (art. 22 OSID) • Protection de base BE recommandée • Mesures de protection supplémentaires adaptées aux risques
	Informations / outils TIC d'autres autorités	Protection de base BE	• Protection de base BE recommandée • Mesures de protection supplémentaires adaptées aux risques prises sous leur propre responsabilité
Sécurité des données	Données personnelles	Protection de base BE	• Protection de base BE recommandée • Mesures de prévention adaptées aux risques (art. 5 OSID) • Analyse des besoins de protection ou concept SIPD basé sur les risques identifiés et les recommandations de l'autorité de protection des données (art. 8 OSID).

Illustration 8 : Champ d'application de la protection de base BE

La protection de base BE étant une instruction de la CNT, elle s'adresse uniquement aux autorités cantonales relevant de son champ d'application, ce qui exclut les tiers mandatés. Les autorités cantonales doivent donc contraindre ces derniers à mettre en œuvre la protection de base BE dans le cadre des conditions générales SIPD BE (CG SIPD BE).

Si le tiers mandaté occupe sur le marché une position l'empêchant de s'acquitter entièrement de cette obligation ou s'il peut garantir la protection de base BE par d'autres mesures de sécurité, il est possible de s'écarter des CG SIPD BE. Les risques qui en découlent doivent être exposés dans l'analyse des besoins de protection et dans le concept SIPD. L'autorité compétente peut par exemple exiger du tiers mandaté qu'il confirme formellement la mise en œuvre de la protection de base BE en joignant à son dossier d'appel d'offres une déclaration sur l'honneur établissant que cette protection demeure garantie malgré les dérogations. Des mesures appropriées doivent être prises pour réduire le risque au niveau accepté.

Article 15 – Détermination des niveaux de protection

Alinéa 1 :

Les objets précieux doivent être protégés en fonction de leur valeur et de ce qui les menace, selon le principe « une place pour chaque chose et chaque chose à sa place ».

Ce principe simple n'est pas toujours facile à mettre en pratique, car il présuppose de dresser un inventaire distinguant les choses de valeur de celles qui n'en ont pas, puis de déterminer le degré de sécurité que nécessitent les premières. Il convient ainsi de définir pour chacun des objets précieux, c'est-à-dire des objets à protéger, le niveau de protection requis en fonction du besoin de protection.

L'annexe 1 de la présente ordonnance expose ce principe pour les trois objets à protéger, à savoir les informations, les données personnelles et les outils TIC. La CNT a pour tâche de préciser dans son instruction sur la protection de base BE les mesures de protection concrètes que les autorités cantonales doivent prendre pour les niveaux de protection 0 et 1. En mettant en œuvre cette instruction, les autorités ont l'assurance que leur sécurité de l'information et des données est conforme aux dispositions légales : une fois que les membres de la direction et leurs spécialistes de la sécurité à chaque échelon ont analysé les risques, défini les mesures de protection sur la base de l'instruction de la CNT et décidé des risques résiduels qu'ils acceptent, ils n'ont plus qu'à veiller à

ce que les mesures définies soient appliquées. Cette procédure permet de garantir que tous les responsables s'acquittent de leurs obligations légales.

Alinéa 2 :

N'appelle aucun commentaire.

Article 16 – Concept SIPD

Alinéa 1 :

Si l'analyse des besoins de protection fait apparaître que l'outil doit satisfaire à des exigences plus élevées que la protection de base, ces exigences doivent être définies dans un concept de sécurité de l'information et de protection des données (concept SIPD). Ce dernier doit aussi spécifier les risques que représentent les éventuelles exigences liées à la protection de base qui ne sont pas remplies, en précisant comment ils sont écartés ou réduits ou s'ils sont acceptés.

Depuis l'entrée en vigueur de l'OD SIPD, le canton de Berne désigne le document qui décrit les mesures de protection excédant la protection de base par le terme « concept SIPD ». L'OD SIPD n'établit pas encore de distinction entre la sécurité de l'information et celle des données. Elle part cependant déjà du principe qu'il ne faut pas uniquement documenter la sécurité de l'information et des données, mais également son impact sur la protection des données ainsi que les mesures de protection à prendre. L'article 19 LCPD désigne désormais cette démarche par le terme « analyse d'impact relative à la protection des données personnelles ». Celle-ci fait ainsi partie intégrante du concept SIPD, qui doit toujours être entendu comme incluant l'analyse d'impact relative à la protection des données.

Tout concept SIPD doit par conséquent au moins exposer :

a) les risques liés au non-respect total ou partiel des exigences relatives à la protection de base ;
b) les mesures de protection particulières prévues au-delà de la protection de base ;
c) les risques résiduels ;
d) l'analyse d'impact relative à la protection des données personnelles, c'est à dire l'évaluation des risques pour les personnes concernées (art. 19, lit. *b* LCPD).

Alinéa 2 :

N'appelle aucun commentaire.

Alinéa 3 :

Le concept SIPD est un instrument central de la sécurité. Il peut notamment se révéler important pour clarifier des violations de la sécurité de l'information et des données, car il indique la manière dont l'autorité a évalué les risques pour les personnes concernées et les mesures qu'elle a prises ou sciemment omises (acceptation des risques). Il doit donc être conservé au moins deux ans après la fin du traitement s'il s'agit d'informations ou de données, ou après la mise hors service s'il s'agit d'outils TIC. Ce délai de conservation s'inspire de l'ordonnance fédérale (art. 14 OPDo).

Article 17 – Tiers mandatés

Alinéa 1 :

Par tiers mandatés, on entend au sens de l'article 6 LSIC et de l'article 12 LCPD toutes les personnes morales ou physiques de droit public ou privé auxquelles l'autorité délègue des tâches légales par contrat. Les bénévoles sont également considérés comme des tiers mandatés, mais sans rémunération.

Actuellement, les principaux tiers mandatés par l'administration cantonale sont Bedag Informatique SA, Swisscom SA et SPIE Suisse SA. Selon l'enquête menée par l'autorité de protection des données du 30 janvier au 15 mars 2026, une large majorité des communes municipales, des paroisses et des communes bourgeoises bénéficient des prestations de Talus SA et Dialog Verwaltungsdata SA, raison pour laquelle ces entreprises ont été associées à l'élaboration de l'OSID.

Alinéa 2 :

Plusieurs incidents survenus chez des tiers mandatés par la Confédération (p. ex. l'incident de sécurité chez Xplain SA) ont montré que ceux-ci doivent respecter les mêmes normes de sécurité que les autorités elles-mêmes lorsqu'ils traitent des informations ou des données personnelles ou fournissent des prestations TIC ; d'où l'importance de fixer des exigences claires concernant la sécurité et son contrôle dans les contrats avec les tiers. Ces contrats doivent inclure l'obligation de garantir la protection de l'information, des données personnelles et des outils TIC conformément aux prescriptions cantonales, et de signaler les incidents de sécurité. De même, ils doivent indiquer les preuves à fournir concernant la mise en œuvre des consignes de sécurité et en particulier réserver un droit d'audit et de contrôle à l'autorité.

À cet effet, la CNT édicte également, en annexe à la Protection de base BE, les CG SIPD BE, publiées sur Internet à l'adresse www.be.ch/cg. Depuis 2015, le Bureau central de coordination des achats (BCCA) propose en outre aux autorités des modèles de contrats disponibles sous www.be.ch/achats.

Il est essentiel que, lorsqu'elles achètent des prestations à des tiers, les autorités intègrent les exigences en matière de sécurité au dossier d'invitation ou d'appel d'offres.

Article 18 – Confirmation de la sécurité de l'information et des données

Il incombe à la haute direction, plus précisément aux responsables de la sécurité des Directions (RS DIR), de décider s'il y a lieu de déployer des efforts supplémentaires pour atténuer ces risques ou si ceux-ci ont déjà été réduits à un niveau accepté.

7.3.2 Gestion de la sécurité de l'information et des données

Article 19 – Risques résiduels et menaces existantes

Alinéa 1 :

Cette disposition précise la responsabilité incombant aux RS, à savoir décider s'ils doivent accepter certains risques résiduels importants et le cas échéant lesquels.

L'autorité compétente pour accepter le risque dépend de la tâche publique concernée. Pour les outils TIC cantonaux, les niveaux de compétences sont détaillés à l'article 32 LAN, qui dispose que l'OIO est responsable de l'acceptation des risques résiduels concernant ses applications de

groupe et les prestations TIC de base. Les autres autorités (Directions, offices, autorités judiciaires, Grand Conseil, autorités de surveillance) assument la responsabilité des risques résiduels liés aux applications spécialisées et aux applications de groupe relevant de leur domaine de compétence. Toutes les autorités répondent en outre de l'acceptation des risques résiduels liés à la manière dont elles utilisent les outils TIC mis à leur disposition par d'autres autorités (p. ex. si un office envoie par courriel des informations dignes de protection sans les crypter).

Comme lors de l'introduction de Microsoft 365, les risques résiduels dont l'étendue ou la portée politique est particulièrement importante doivent néanmoins pouvoir être évalués et acceptés par la direction politique compétente ou, pour ce qui est des risques relevant de la responsabilité des DIR/CHA, par le Conseil-exécutif en sa qualité de haute direction de l'administration cantonale. Il appartient aux autorités compétentes d'apprécier, selon des critères techniques et politiques, les cas nécessitant leur intervention.

Les RS des DIR/CHA/PARL/JUS peuvent ainsi soumettre ces risques à l'acceptation de leur responsable hiérarchique comme suit :

a) RS DIR ou Office : à la directrice ou au directeur de la Direction concernée, ou à la chancelière ou au chancelier d'État ;
b) RS DIR du Grand Conseil : au Bureau du Grand Conseil ;
c) RS DIR des autorités judiciaires et du Ministère public : à l'organe désigné à cet effet par ces derniers.

Alinéa 2 :

N'appelle aucun commentaire.

Article 20 – Système de management de la sécurité de l'information

Alinéa 1 :

Un système de management de la sécurité de l'information (SMSI) comprend les procédures et les règles qui définissent la manière dont la sécurité de l'information et des données est organisée dans un système et permet de visualiser les tâches, compétences et responsabilités attribuées aux différentes fonctions. Tandis que la CNT est chargée de concevoir et de garantir le bon fonctionnement, le contrôle et l'amélioration constante du SMSI du canton, l'exploitation opérationnelle de ce système relève de la compétence du service de conseil SID, en collaboration avec les CS des autorités cantonales. En vertu de l'article 41, alinéa 1, le SMSI cantonal doit être mis en service dans les deux ans suivant l'entrée en vigueur de l'OSID. Il est exploité par le service de conseil SID et repose sur les exigences de la norme ISO/IEC 27001.

Un SMSI a pour but de guider chaque autorité dans la mise en œuvre et l'amélioration de la sécurité de l'information et des données en son sein. Ce processus implique de définir des objectifs concrets, qui permettent aussi au Conseil-exécutif d'évaluer si le système produit les effets souhaités. Il appartient à la CNT de fixer ces objectifs et de mesurer leur degré de réalisation ; elle définit les objectifs du SMSI et vérifie chaque année s'ils sont atteints en collectant les indicateurs nécessaires.

Alinéa 2 :

Afin que l'évaluation de la mise en œuvre et de l'efficacité du SMSI soit relativement objective et comparable, cette disposition exige un contrôle périodique par un organe indépendant de l'autorité ou une instance supérieure. Ce contrôle indépendant garantit l'amélioration constante de la sécurité, tout en assurant la confiance des partenaires de l'autorité. Il appartient à la CNT, en sa qualité

de responsable du SMSI, de décider de la manière dont elle entend gérer les résultats de ce contrôle et de définir les mesures de protection à prendre. L'amélioration continue du système est fondamentale pour garantir la sécurité. Les contrôles permettent d'assurer ce processus. Si la périodicité de trois ans est calquée sur le cycle de certification officiel de la norme ISO (ISO/IEC 27001), l'étendue du contrôle prescrit est moins ambitieuse que celle de cette norme. En effet, le contrôle ne comprend pas obligatoirement un audit formel au sens de la norme ISO : selon le mandat, il peut porter sur l'ensemble du SMSI ou uniquement sur certains de ses éléments. Le choix de l'organe indépendant revient à la CNT, qui peut confier ces contrôles au Contrôle des finances, à l'autorité cantonale de protection des données ou à des tiers.

Article 21 – Inventaire des objets à protéger

Alinéa 1 :

L'inventaire défini ici recense l'ensemble des objets à protéger (art. 3, lit. *b* OSID), c'est-à-dire des informations, des données personnelles et des outils TIC, à une date déterminée. Dans la mesure du possible, il doit être dressé dans les applications de groupe existantes.

L'administration cantonale dispose d'ores et déjà d'un système de gestion des services informatiques (ITSMS) qui répertorie, avec le niveau de protection correspondant, toutes les applications, par exemple l'application de la DTT BExpert (lien vers le système ITSMS, accessible uniquement pour les collaboratrices et collaborateurs de l'administration cantonale assumant un rôle TIC). Dans l'ITSMS, le niveau de protection 0 est attribué à cette application, ce qui correspond à la protection de base. Le besoin de protection doit être déterminé pour chacun des outils TIC conformément à l'article 33 OSID.

L'inventaire des fichiers de données personnelles – qui sont pratiquement toujours des outils TIC – comprend quant à lui les fichiers devant être annoncés en vue de leur inscription dans le registre en application de l'article 21 LCPD. Il contient également les fichiers de données personnelles exclus de l'obligation d'annoncer visée à l'article 21, alinéa 4 LCPD, étant donné que les demandes de renseignements visées à l'article 29 LCPD s'étendent aussi aux fichiers de données non enregistrés.

Alinéa 2 :

N'appelle aucune remarque.

Alinéa 3 :

La CNT définit les indications à fournir dans l'inventaire, par exemple :

a) le besoin de protection des objets à protéger,
b) l'autorité cantonale responsable des objets à protéger et la personne ou fonction compétente en la matière,
c) la participation de tiers mandatés,
   La liste des tiers liés par un contrat, par exemple les fournisseurs de prestations informatiques, permet d'une part de faciliter la gestion des prestataires et de repérer en amont tout lien de dépendance entre eux (ainsi que d'évaluer les risques de concentration qui en découlent) et, d'autre part, d'identifier les risques que ces prestataires font courir à l'autorité,
d) le niveau de protection déterminé,
e) la mise en œuvre des mesures correspondant au niveau de protection.

Elle ne doit pas forcément être documentée dans l'inventaire lui-même, mais celui-ci doit au moins indiquer le lieu où sont conservés les documents relatifs à la sécurité, et la personne qui en est responsable,

f) les contrôles et les audits périodiques,
g) la date de la dernière mise à jour de l'inventaire.

Article 22 – Mesures de protection d'objets à protéger utilisés par des tiers

Alinéa 1 :

Cette disposition règle les cas dans lesquels des tiers utilisent des objets à protéger du canton à des fins légitimes qui leur sont propres (à distinguer des traitements de données confiés à des tiers par les autorités cantonales, pour lesquels la sécurité doit être définie contractuellement). Il appartient à l'autorité cantonale de décider du type de réglementation approprié (instruction, décision, contrat de droit public ou de droit privé), en fonction du contexte. En l'absence de base juridique spécifique, les éventuels contrats de droit public reposent sur l'article 25 LAN. Ces contrats peuvent par exemple revêtir la forme de conditions d'utilisation des outils TIC cantonaux devant impérativement être acceptées pour pouvoir utiliser les outils en question. Selon les risques en présence, la réglementation peut aussi régler le contrôle de la mise en œuvre des mesures et les sanctions applicables en cas de non-respect, comme le blocage de l'accès ou une peine conventionnelle.

Alinéa 2 :

Afin de s'assurer, comme le veut le canton, que les objets à protéger soient gérés selon des exigences de sécurité au moins équivalentes à celles prévues par la LSI, il est indispensable de laisser aux autorités fédérales la possibilité d'édicter des prescriptions spécifiques à leurs propres objets si le droit fédéral ne leur en attribue pas déjà la compétence. Le canton ne peut cependant pas obliger les autorités fédérales à faire usage de cette possibilité. Si elles y renoncent, l'article 3 LSI permet de contraindre les tiers qui utilisent des objets à protéger de la Confédération d'appliquer directement la LSI et ses dispositions d'exécution. L'alinéa 2 a donc un caractère purement déclaratoire.

Article 23 – Dérogations aux prescriptions

Cette disposition explicite le principe selon lequel les mesures de protection dépendent des risques en présence et précise qu'il revient à la ou au RS compétent pour l'objet à protéger de décider des risques à accepter. La personne dirigeante responsable des risques peut ponctuellement s'écarter des mesures de protection prescrites dans un acte législatif ou une instruction (p. ex. la Protection de base BE) si elle parvient à la conclusion documentée et motivée que les coûts de la mesure en question ou ses autres inconvénients pour l'exécution des tâches des autorités sont disproportionnés par rapport à la réduction des risques visée, et qu'elle accepte le risque résiduel.

Ces dérogations aux prescriptions de sécurité doivent être limitées dans le temps, afin de contraindre à effectuer des contrôles réguliers, et documentées, motivation à l'appui, dans l'une des applications de groupe mises à disposition par le service de conseil SID.

Leurs conséquences pouvant toucher les objets de plusieurs autorités, il appartient en principe à la chargée ou au chargé de sécurité de la CNT (CS CNT) de les approuver. Par exemple : En assouplissant une mesure de protection concernant l'accès à son application spécialisée, une autorité peut accroître le risque de cyberattaques contre d'autres autorités, via le réseau cantonal. Sa décision doit donc préalablement faire l'objet d'une évaluation des risques à l'échelon supérieur. Mais si une mesure concerne en réalité les objets à protéger d'une seule et même autorité, la ou le CS CNT peut laisser le soin d'en décider à la ou au RS compétent.

Article 24 – Assistance en cas d'incident de sécurité

Lorsqu'ils ont adopté la LSIC, le Grand Conseil et la Commission des institutions politiques et des relations extérieures (CIRE) étaient conscients qu'elle risquait d'entraîner des charges supplémentaires pour les autres autorités, notamment les communes. Ils ont néanmoins exigé de l'administration cantonale qu'elle mette à disposition des possibilités de formation (art. 19, al. 2 LSIC), proposées contre rémunération. Cet article exclut toute offre de service direct de conseil et d'assistance en cas d'incident de sécurité aux autres autorités.

Le service de conseil SID limite donc son assistance directe aux autorités cantonales, compte tenu de ses ressources. S'il ne dispose pas des moyens nécessaires à cet effet, il peut bénéficier des prestations incluses dans les différents contrats-cadres, pour autant que l'autorité cantonale sollicitée ait octroyé une garantie de prise en charge des frais correspondants.

En cas d'incident, l'autorité cantonale concernée suit le processus « Major-Security-Incident » (lien vers Adonis, dont l'accès est réservé au personnel cantonal) déjà défini aujourd'hui pour gérer les incidents de sécurité survenant au niveau interdirectionnel, qui attribue au rôle actuel de DSI (futur CS CNT) une fonction dirigeante.

Les autres autorités peuvent elles aussi conclure à leurs frais des contrats individuels à des conditions avantageuses auprès de prestataires de services qualifiés. Des informations à ce sujet sont disponibles sur le site Internet de la Centrale d'achat cantonale TIC de l'OIO (www.be.ch/achats).

Article 25 – Contrôles et audits

Les contrôles et les audits permettent aux autorités de se rendre compte du respect des prescriptions en matière de sécurité, de l'efficacité des mesures de protection et des mesures de corrections nécessaires. C'est la raison pour laquelle l'article 5, alinéa 1, lettre *d* LSIC dispose que la sécurité de l'information doit faire l'objet de contrôles réguliers. En renvoyant à la LSIC, l'article 10, alinéa 2 LCPD étend ce principe aux données personnelles.

Cet article contraint par conséquent les autorités cantonales à définir chaque année les contrôles et audits basés sur les risques qu'elles entendent réaliser l'année suivante et pour quelles raisons. L'approbation du plan d'audits et des ressources nécessaires incombe aux RS DIR de l'autorité concernée : le nombre de contrôles et d'audits devant être effectués chaque année n'est donc pas fixe, mais laissé à l'appréciation des RS DIR, qui prennent cette décision sur la base de leur évaluation des risques.

Étant donné que le Contrôle des finances et l'autorité de protection des données vérifient eux aussi périodiquement la sécurité de l'information et des données, les RS DIR doivent se coordonner avec le service de conseil SID, qui évalue les besoins de contrôle et d'audit en collaboration avec l'autorité cantonale de protection des données et le Contrôle des finances, s'entretient chaque année avec eux et connaît leurs plans d'audit. Le service de conseil SID peut par ailleurs mener lui-même des audits. Cela permet de garantir que les audits sont efficaces et économes et basés sur les risques et ainsi d'éviter aux autorités auditées et à leurs mandataires des contrôles répétés de même contenu, sans aucune coordination.

Article 26 – Rapports

Alinéas 1 à 3 :

L'amélioration à long terme de la sécurité de l'information et des données implique un contrôle continu de son efficacité ainsi qu'une adaptation constante des mesures de protection. Cet article

prescrit donc la rédaction d'un rapport annuel sur l'état de la sécurité de l'information et des données qui doit être soumis à l'appréciation de la CNT, qui est responsable du pilotage de la sécurité. Les RS DIR et leurs CS fournissent les indications nécessaires à la ou au CS CNT, qui remet le rapport à la CNT.

Il indique en particulier :

a) l'état et l'efficacité du SMSI des autorités cantonales,
b) l'avancement de la mise en œuvre des mesures de protection,
c) l'acceptation des risques résiduels particulièrement importants par les RS DIR ou le Conseil-exécutif,
d) les mesures de sensibilisation mises en œuvre,
e) les conclusions tirées des incidents et failles de sécurité,
f) les conclusions des contrôles et des audits,
g) les mesures d'amélioration prises et proposées.

Alinéa 4 :

Le rapport contient des informations sensibles, qui doivent donc être classifiées « CONFIDENTIEL ». Il est impératif d'établir par voie d'ordonnance, de manière univoque et sans déroger à l'évaluation des risques, que le rapport de la CNT ne peut être communiqué qu'à un cercle restreint de destinataires clairement désignés. Ce groupe comprend au plus :

a) le Conseil-exécutif,
b) les RS DIR concernés,
c) l'autorité cantonale de protection des données,
d) le Contrôle des finances,
e) le service spécialisé de la Confédération pour la sécurité de l'information visé à l'article 83 LSI.

7.3.3 Classification d'informations

La classification est obligatoire dans la mesure où les critères énoncés aux articles 27 ss OSID sont remplis. Le principe du besoin d'en connaître au sens de l'article 9, alinéa 1, lettre *b* LSIC s'applique. Comme indiqué sous chiffre 3.5 ci-dessus, intitulé « Objectifs d'effet », la LSIC et l'OSID visent cependant également à ce que les classifications se raréfient et soient désormais exclusivement fondées sur des critères clairs. L'objectif est de diminuer aussi bien la quantité des informations classifiées que la durée de la classification.

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 des intérêts publics définis à l'article 1, alinéa 2, lettres *a* et *b* LSIC. Il en va de même pour les informations qui sont traitées par les tribunaux ou 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 requise en vertu de la LSIC. En revanche, les mesures particulières prises pour protéger ces informations peuvent être classifiées (p. ex. un concept SIPD ; voir aussi le rapport relatif à la LSIC du 16 août 2023 concernant l'art. 8, al. 1). De même, la détermination du besoin de protection des outils TIC prévue à l'article 33 OSID protège les données personnelles.

Article 27 – Catalogues de classification

Alinéa 1 :

Les membres de la haute direction les mieux à même d'évaluer quel type d'information relevant de leur domaine de compétence constitue régulièrement un intérêt à protéger sont les RS DIR. C'est donc à eux que l'alinéa 1 confie la tâche d'établir un catalogue de classification répertoriant le plus exhaustivement possible les informations relevant de leur domaine de responsabilité. Ce catalogue doit également indiquer pour quelle durée est prévue la classification. Les informations à classifier étant régulièrement traitées dans le cadre des tâches effectuées, il est la plupart du temps possible de déterminer à l'avance jusqu'à quand elles doivent rester classifiées à un échelon ou à un autre. La LSIC ne définit pas de délai minimal ni maximal.

Alinéa 2 :

Cette vérification vise à garantir dès l'élaboration des catalogues de classification que l'application des critères légaux de classification utilisés par les autorités cantonales s'appuie sur des règles comparables. La décision finale revient aux RS DIR.

Alinéa 3 :

Certains types d'information étant traités dans l'ensemble ou dans la plupart des autorités (p. ex. informations sur les outils TIC, les affaires du Conseil-exécutif ou les zones de sécurité au sens de l'art. 18 LSIC), leur classification doit être régie de manière uniforme pour toute l'administration. Élaboré par la ou le CS CNT en collaboration avec les CS DIR, ce catalogue de classification général est ensuite soumis pour décision à la CNT. Il doit définir comment les informations doivent être classifiées et pour combien de temps.

Le service de conseil SID élaborera des modèles de catalogue.

Article 28 – Instructions de classification et d'exécution

Alinéas 1 et 2 :

Les collaboratrices et collaborateurs sont tenus de se conformer aux catalogues de classification pour classifier les informations qu'ils répertorient, en apposant la mention correspondante. Étant donné que les catalogues ne sont pas exhaustifs, il peut toutefois arriver que des collaboratrices et des collaborateurs considèrent une information comme digne de protection, mais ne la trouve pas dans le catalogue. Le cas échéant, ils sont tenus soit de la faire ajouter dans le catalogue soit de la classifier directement sur la base des critères visés aux articles 29 et suivants OSID. Cette même obligation s'applique aussi aux organes des autorités mandantes qui confient à des tiers le traitement d'informations ou de données personnelles devant être protégées.

Pour s'assurer que les personnes utilisant un objet à protéger se rendent immédiatement compte de son besoin de protection et le traitent en conséquence, les documents et autres supports d'information contenant des informations classifiées doivent être munis de l'une des mentions de classification suivantes, écrite en majuscules : « INTERNE », « CONFIDENTIEL » ou « SECRET » ; la classification des informations dignes de protection doit également être précisée lors des échanges oraux.

Alinéa 3 :

Jusqu'ici, l'édiction de prescriptions de traitement relevait de la responsabilité de la CHA, qui a notamment rédigé l'article 8 « Prescriptions de traitement » de l'OCACE. Désormais, cette compétence sera reprise par la CNT, qui compte des membres de la CHA. La ou le CS CNT fera en particulier appel à cette dernière lors l'élaboration des prescriptions de traitement. La procédure prévue s'inspire de la solution uniformisée de la Confédération en matière de prescriptions de traitement, qui décrit non seulement les informations classifiées, mais aussi leur identification au moyen de la mention de classification, y compris en cas de déclassification. Confier le règlement de ces tâches à deux autorités distinctes compliquerait considérablement la mise en œuvre des instructions par le personnel, ce qui nuirait à l'effet de la classification et, partant, à la reconnaissance de l'équivalence par la Confédération.

Article 29 – Classification « INTERNE »

Fondées sur les types d'intérêts publics définis à l'article 1, alinéa 2, lettres *a* et *b* LSIC en général, les règles de classification s'inspirent plus particulièrement de celles de la Confédération, transposées aux tâches et aux risques propres au canton.

Le critère permettant de déterminer si une information doit être classifiée ou non est la présence d'indices qualifiés susceptibles de justifier au moins la classification « INTERNE ». Il ne suffit pas que la divulgation de l'information soit susceptible de causer un simple dommage négligeable : l'atteinte pouvant être portée aux intérêts doit être notable. Lorsqu'il s'agit d'informations touchant l'ordre public et la sécurité (art. 1, al. 2, lit. *b* LSIC), le seuil de classification « INTERNE » peut relativement vite être atteint. C'est la classification la plus courante dans de tels cas. Ainsi, les divers documents relatifs à la sécurité des outils TIC ou de simples plans d'engagement des forces d'intervention sont classifiés « INTERNE ».

Il convient de rappeler à cet égard que la classification n'est pas déterminante pour la communication ou non d'informations sur demande dans le cadre du principe de publicité (art. 27 ss de la loi du 2 novembre 1993 sur l'information et l'aide aux médias [LIAM][29]). En effet, la LIAM prévaut sur la LSIC (art. 3, al. 1 LSIC). Ainsi, peser les intérêts au sens des articles 27 et suivants LIAM s'impose même pour les documents classifiés. La classification donne cependant un indice qu'il existe des intérêts publics importants plaidant contre une publication.

Article 30 – Classification « CONFIDENTIEL »

Par rapport à la classification « INTERNE », la classification « CONFIDENTIEL » répond à une exigence de protection plus élevée. Elle implique un dommage clair et considérable.

Article 31 – Classification « SECRET »

Sont classifiées « SECRET » les rares informations dont la divulgation est susceptible d'entraîner des dommages particulièrement importants pouvant avoir des conséquences catastrophiques pour certaines autorités ou personnes. Cette classification n'est utilisée que dans des cas exceptionnels : d'une part, parce qu'il existe peu d'informations dont la divulgation risque d'entraîner des dommages d'une telle ampleur et, d'autre part, parce que le traitement de cette catégorie d'informations nécessite de lourdes mesures de protection.

En vertu des prescriptions de traitement édictées par la Confédération en annexe à son ordonnance concernant la protection des informations (OPrI)[30], les informations de ce genre ne peuvent

[29] LIAM, RSB 107.1
[30] OPrI, RS 510.411

être traitées qu'avec des outils TIC dotés d'une protection particulière, le supports sur lequel elles sont enregistrées doit être numéroté et enregistré, leur transmission électronique doit se faire par cryptage renforcé et être traçable, leur communication orale doit avoir lieu uniquement dans des lieux protégés contre les écoutes et leur remise physique n'être effectuée qu'en main propre ou par courrier spécial contre délivrance d'une quittance, etc.

Article 32 – Déclassification et extinction de la classification

Alinéas 1 et 2 :

Le but déclaré de la LSIC et de l'OSID est de réduire considérablement la quantité d'informations classifiées (voir ch. 3.5), une tâche qui incombe aux autorités cantonales tenues de protéger et de classifier les informations. C'est à elles, ou plus précisément à leurs collaboratrices et collaborateurs, qu'il appartient de vérifier le besoin de protection tant des objets figurant dans le catalogue de classification que des informations classifiées, et d'adapter leur classification, voire de les déclassifier, si les conditions requises ne sont plus réunies (voir aussi art. 28, al. 1 OSID).

La vérification s'impose non pas en permanence ou à intervalles réguliers, mais uniquement dans des cas particuliers, comme la clôture d'une affaire ou la demande d'accès à des informations des autorités (demandes formelles ou informelles d'accès à des informations au sens des art. 27 ss LIAM). Elle relève de la seule compétence de l'autorité qui a évalué le besoin de protection de l'information et déterminé la classification en conséquence.

Les classifications limitées dans le temps (p. ex. « CONFIDENTIEL jusqu'au 1.1.2030 ») s'éteignent au terme du délai prescrit sans nécessiter l'actualisation de la mention de classification ni aucune autre action de la part de l'autorité compétente.

Alinéa 3 :

Comme indiqué à l'article 9, alinéa 2 LSIC, l'accès à des archives classifiées est régi par les dispositions de la législation sur l'archivage et notamment, dans le présent contexte, par celles relatives aux délais de protection ordinaires et particuliers (voir art. 17 et 18 de la loi du 31 mars 2009 sur l'archivage [LArch][31]). En renvoyant aux délais de protection prévus par la législation sur les archives, le législateur a tenu compte du fait que le maintien du secret perdait son importance au fil du temps et a établi, dans une mise en balance anticipée des intérêts, qu'au terme du délai de protection, l'intérêt de garder le secret ne primait plus celui de consulter l'information concernée (Rapport du Conseil-exécutif à l'attention du Grand Conseil concernant la loi sur l'archivage, *in* Journal du Grand Conseil 2009, annexe n° 14, p. 5).

Au cours du délai de protection, la classification fait partie des éléments à considérer dans la mise en balance des intérêts visée aux articles 27 et suivants LIAM (voir commentaire de l'art. 3 LSIC dans le rapport du 16 août 2023), qui s'impose du fait du renvoi de l'article 16, alinéa 1 LArch à la LIAM. Selon le droit en matière d'archivage, l'intérêt de garder le secret ne s'oppose plus à la consultation de l'information concernée au terme du délai de protection.

L'article 32 OSID transpose ces principes à la classification et précise que celle-ci s'éteint automatiquement à l'échéance des délais de protection prévus par la législation sur les archives, rendant par là-même les informations librement accessibles.

[31] LArch, RSB 108.1

7.3.4 Détermination du besoin de protection des outils TIC

Article 33 – « Protection de base », « protection élevée » et « protection très élevée »

Alinéa 1 :

Le besoin de protection d'un objet est déterminé par les intérêts publics du canton au sens de l'article 1, alinéa 2, lettres *a* à *c* LSIC. Globalement, les critères matériels présidant à la définition du besoin de protection des informations et des données personnelles s'appliquent aussi aux outils TIC. Contrairement à la classification des informations, la définition des besoins de protection des outils TIC est en plus guidée par des critères d'ordre financier. Une violation de la disponibilité ou de l'intégrité d'informations traitées au moyen d'outils TIC est plus facile à quantifier que, par exemple, une violation de la confidentialité d'un document contenant des informations classifiées.

Lettre *b,* chiffre 4 :

Alors que l'article 30, alinéa 1, lettre *d* OSID protège avant tout les intérêts publics visés à l'article 1, alinéa 2, lettre *b* LSIC, c'est-à-dire l'ordre public et la sécurité, l'article 33, alinéa 1, lettre *b*, chiffre 4 protège par exemple les données personnelles d'un agent infiltré ou d'enfants menacés d'enlèvement par un parent séparé, autrement dit des intérêts individuels.

Alinéa 2 :

Les autorités doivent aussi systématiquement vérifier le besoin de protection des outils TIC ayant été modifiés. Le cas échéant, il convient d'adapter en conséquence l'analyse des besoins de protection et éventuellement le concept SIPD. Une nouvelle menace ou une menace récurrente peut toutefois aussi suffire à remettre en question la totalité ou une partie d'une analyse de risques, et ainsi potentiellement nécessiter une modification du concept SIPD.

C'est ce qui explique que les outils TIC dont le besoin de protection est défini doivent faire l'objet d'une procédure de sécurité au moins tous les deux ans. Contrairement à la Confédération, le Conseil-exécutif renonce cependant à l'obligation de soumettre périodiquement les outils TIC présentant un besoin de protection de base à la procédure de sécurité, estimant que le risque en présence ne justifie pas le travail nécessaire, ne serait-ce que pour les centaines d'applications de groupe entrant dans la catégorie « Protection de base » : l'administration cantonale compte un total de plus de 1400 applications, dont quelque 700, soit 50 % présentent un besoin de protection 0 ou 1, soit la protection de base (ITSMS, état : juillet 2026).

7.3.5 Personnes à contrôler

En raison de son atteinte aux droits individuels des personnes concernées, le contrôle de sécurité relatif aux personnes est déjà réglé de manière détaillée dans la loi aux articles 19 et suivants LSIC. C'est pourquoi nous renvoyons également ici aux passages correspondants du rapport sur la LSIC, chiffre 8.6.2. L'OSID n'en régit que les aspects relatifs à leur exécution exposés ci-après.

Article 34

En vertu de l'article 23 LSIC, la décision relative aux personnes à contrôler et au mode de contrôle ne doit pas dépendre de l'évaluation individuelle des risques par l'autorité responsable, mais reposer sur une liste répertoriant les fonctions à contrôler.

Alinéa 1 :

Conformément au principe selon lequel la sécurité de l'information et des données est l'affaire des dirigeantes et dirigeants, il appartient au Conseil-exécutif de désigner, parmi les personnes qu'il a nommées, celles qui doivent être soumises à un contrôle de sécurité (CSP). La Direction des finances prépare cette décision après consultation de la CNT et de la Conférence des secrétaires généraux (CSG). La CNT étant l'organe de l'administration spécialisé dans les risques liés à la sécurité de l'information et des données, et la CSG celui de la haute direction, leurs compétences sont essentielles pour établir la liste des fonctions de haute direction nécessitant un CSP.

Alinéa 2 :

La règle selon laquelle il incombe à la CSG de désigner les fonctions de direction et le personnel subalternes devant être soumis à un CSP repose sur des considérations analogues : la CNT, en sa qualité d'organe TIC suprême, doit contribuer à définir les fonctions TIC à inscrire sur la liste.

Alinéa 3 :

Les fonctions dont la responsabilité et les risques exigent un CSP sont des positions clés susceptibles d'être la cible de cyberattaques ou d'autres actes offensifs. Au-delà des personnes concernées, ce sont donc aussi des intérêts importants du canton de Berne qui se trouvent menacés. C'est la raison pour laquelle la liste n'est pas publiée.

7.4 Organes chargés de la sécurité

Avec l'OAN, le Conseil-exécutif a institué des organes de pilotage et de gestion de la transformation numérique et des TIC dont certains chapeautent non seulement le canton dans son ensemble (y compris les affaires des communes et les organisations autonomes chargées de tâches publiques) mais aussi l'administration cantonale. Étant donné que les questions de sécurité de l'information et des données se posent avant tout en lien avec les systèmes TIC et les projets de numérisation, l'article 31, alinéa 2 LSIC habilite le Conseil-exécutif à déléguer celles de portée cantonale et celles de l'administration cantonale aux organes prévus par la LAN et l'OAN, afin d'éviter de mettre sur pied deux organisations distinctes chargées de la sécurité de l'information et des données, comme l'a fait la Confédération, par exemple. Cela facilite la prise en compte de la sécurité comme composante de la transformation numérique de l'administration publique et permet donc d'éviter l'institution de nouveaux organes spécialisés, plus onéreux.

Les autres autorités – notamment les communes municipales, les paroisses et les communes bourgeoises – doivent se doter de leur propre organisation de sécurité, adaptée à leurs tâches et à leurs risques, et désigner au moins une personne disposant d'une formation adéquate ainsi que des compétences et des ressources appropriées pour assumer la responsabilité de la sécurité de l'information et des données (art. 32 LSIC).

L'organisation de la sécurité se compose des organes ci-après (voir aussi le graphique sous ch. 3.4).

Article 35 – Conférence pour l'administration numérique et les TIC

Alinéa 1 :

À l'échelle du canton, le pilotage et la gestion des activités relatives à la sécurité de l'information de l'administration relèvent de la compétence de la CNT et de son groupe spécialisé Sécurité de l'information et des données (groupe spécialisé SID). Ce sont eux qui édictent notamment les documents de référence en matière de sécurité, telles les instructions ou les aides à l'exécution.

La CNT édicte également, entre autres, des instructions précisant les éléments suivants :

a) protection de base BE,
b) objectifs du SMSI,
c) gestion de la sécurité de l'information et des données,
d) niveaux et mesures de protection applicables aux objets à protéger,
e) définition du besoin de protection des objets à protéger par les autorités cantonales,
f) utilisation des objets à protéger dont le besoin de protection a été défini,
g) mesures techniques,
h) mesures physiques,
i) contrôle de l'identité de personnes et de systèmes,
j) système de gestion des identités et des accès (Identity- and Access-Management-System, système IAM).

Dans cette tâche, la CNT est assistée par la ou le CS CNT, qui dirige également le service de conseil SID et le domaine spécialisé Sécurité de l'OIO. Elle ou il est désormais membre de la CNT (voir à ce sujet la modification indirecte de l'art. 18, al. 1 OAN).

Alinéa 2 :

En collaboration avec l'autorité cantonale de protection des données, la CNT tient une liste, régulièrement mise à jour, des nouvelles technologies selon l'article 18, alinéa 2 LCPD entraînant un risque élevé pour les personnes qui les utilisent pour traiter des données personnelles et pouvant donc nécessiter un contrôle préalable au sens de l'article 20, alinéa 1, lettre *b* LCPD. Jusqu'ici, cette liste figurait dans l'OPD. La pratique ayant cependant révélé qu'en raison de l'évolution de la technique, cet outil d'aide à l'exécution se périmait rapidement, par exemple parce qu'il n'intégrait pas de nouvelles technologies aux risques élevés, il est désormais géré au niveau de l'administration.

Alinéa 3 :

N'appelle aucun commentaire.

Alinéa 4 :

L'ordonnance prévoit de déléguer certains documents au groupe spécialisé SID, par exemple les annexes techniques à l'instruction sur la protection de base BE (art. 31, al. 2 LSIC).

Article 36 – Responsables de la sécurité

Alinéa 1 :

Au niveau hiérarchique le plus élevé des autorités cantonales (DIR/CHA/JUS, Grand Conseil et autorités de surveillance, regroupés ci-après sous l'appellation « niveau de la Direction »), la responsabilité de la sécurité de l'information et des données revient à la personne dirigeante la plus haut placée n'ayant pas été élue par le peuple, qui exerce ainsi le rôle de responsable de la sécurité au niveau de la Direction (RS DIR). Il s'agit des secrétaires généraux, de la chancelière ou du chancelier d'État ainsi que des cheffes et chefs des autorités de surveillance. La cheffe ou le chef de l'OIO assume les tâches de RS DIR pour la fourniture des prestations TIC de base et les applications de groupe de l'office, car, dans l'organisation TIC de l'administration cantonale, l'OIO est assimilé à une Direction.

Selon l'article 32 LSIC, les autorités qui n'appartiennent pas à l'administration cantonale se dotent d'une organisation de la sécurité. C'est notamment le cas des autorités judiciaires et du Ministère public. Étant donné que les RS DIR accomplissent des tâches relevant de l'organisation de la sécurité à l'échelle du canton, par exemple en exerçant la fonction d'interlocuteur de la ou du CS CNT, et qu'en vertu de la LAN la justice utilise les TIC cantonaux, il convient de préciser, en application de l'article 31 LSIC, que la Direction de la magistrature doit confier ce rôle à une personne dirigeante capable d'assumer la responsabilité qui en découle. Pour le surplus, elle se dote de sa propre organisation en la matière.

Alinéa 2 :

Dans les offices des DIR/CHA, la responsabilité en matière de sécurité de l'information et des données incombe aux cheffes et chefs d'office, qui exercent le rôle de responsable de la sécurité au niveau de l'office (RS Office). La justice ayant sa propre organisation, il appartient à la Direction administrative de la magistrature de décider pour les autorités judiciaires et le Ministère public s'il convient également de désigner une ou un RS Office par exemple pour le Ministère public ou pour certains tribunaux. La responsabilité se répartit entre les RS Office et la ou le RS DIR du fait de leur lien de subordination, les RS DIR exerçant ainsi la surveillance en matière de sécurité. La ou le RS DIR et les RS Office sont ainsi coresponsables de la sécurité des offices. L'OIO, dont la direction assume le rôle de RS DIR, fait exception à cette règle.

Alinéa 3 :

Les personnes dirigeantes mentionnées aux alinéas 1 et 2 peuvent déléguer la responsabilité en matière de sécurité et les tâches et compétences afférentes à une fonction qui leur est directement subordonnée. Cette démarche peut par exemple se révéler judicieuse lorsque la personne délégataire dispose de connaissances techniques particulières dans le domaine de la sécurité de l'information ou des TIC.

Alinéa 4 :

Les RS assument la responsabilité générale de la sécurité de l'information et des données dans leur domaine de compétence. Cette responsabilité fait partie de leur rôle de hautes dirigeantes et hauts dirigeants et ne peut être déléguée qu'aux conditions susmentionnées. Leurs tâches relèvent aussi bien du domaine de la sécurité que des fonctions de direction.

Lettre *a* : les RS prennent toutes les décisions qui ont une influence déterminante sur la sécurité de l'information et des données relevant de leur domaine de compétence, notamment en ce qui concerne l'organisation, les processus, l'acceptation des risques et les objectifs en matière de sécurité.

a) Ils engagent les mesures de protection nécessaires, notamment en matière de formation et de sensibilisation.
b) Sur proposition de leurs CS et en accord avec le service de conseil SID, ils adoptent le plan annuel de contrôles et d'audits (art. 25, al. 1 OSID).
c) Ils garantissent la mise en place, l'exploitation, la vérification et l'amélioration constante du SMSI dans leur domaine de compétence.

Lettre *b* : les cadres supérieurs tels les RS ne disposant généralement pas de connaissances spécifiques en sécurité de l'information et des données, ils sont assistés par des chargées ou chargés de sécurité (CS). Il appartient aux RS de choisir les CS, de les diriger et de leur fournir les ressources nécessaires, Ils doivent les sélectionner en veillant à ce qu'ils disposent des qualifications requises, à l'instar des autorités visées à l'article 32, alinéa 2 LSIC.

Article 37 – Chargées ou chargés de sécurité

En sa qualité de spécialiste, la ou le CS garantit la réalisation des tâches opérationnelles liées à la sécurité de l'autorité concernée et soutient la ou le RS. Les CS fournissent l'expertise en matière de sécurité de l'information et des données dans leur unité administrative. Cette tâche requiert les qualifications suivantes, en particulier en ce qui concerne les CS DIR :

a) diplôme fédéral d'une école professionnelle ou d'une haute école spécialisée dans la sécurité de l'information et des données ;
b) expérience professionnelle dans la sécurité de l'information et des données, la protection des données ou la gestion du risque ;
c) expérience professionnelle dans la mise en œuvre ou le suivi de projets dans le domaine des TIC ou de la sécurité de l'information et des données.

Il est possible de se procurer les connaissances techniques nécessaires auprès d'expertes ou experts externes. L'OIO met d'ores et déjà à la disposition de l'administration cantonale des contrats-cadres permettant de bénéficier de prestations en matière de sécurité de l'information et des données (www.be.ch/CAC).

Pour éviter tout conflit d'intérêts, il est préférable que les CS ne soient pas subordonnés aux responsables des TIC ni n'assument des tâches liées à l'exploitation de ces dernières.

Alinéa 1 :

La CNT, qui assure le pilotage de la sécurité de l'information et des données, dispose également d'une ou d'un CS. Le canton ne disposant pas des ressources en personnel suffisantes pour instituer deux centres de compétences cantonaux pour la sécurité de l'information en parallèle, la direction du domaine de l'OIO spécialisé dans la sécurité, à savoir le service de conseil SID, assume aussi le rôle de CS CNT. Il faut se résoudre à ce que cette fonction soit subordonnée à la ou au RS OIO, d'une part parce qu'elle serait rattachée à une ou un RS DIR même si elle occupait une autre place dans l'organigramme et, d'autre part, parce que ses tâches se limitent au conseil et à la coordination et excluent toute surveillance susceptible de créer un conflit d'intérêts avec son rôle au sein de l'OIO. La surveillance de la sécurité de l'information et des données incombe à l'autorité de protection des données et, le cas échéant, au Contrôle des finances, les deux autorités de surveillance indépendantes de l'administration compétentes en la matière.

Alinéa 2 :

Lettre *a* : il est possible et parfois même judicieux qu'une même personne exerce le rôle de CS pour plusieurs offices de la Direction, voire, en plus, pour la Direction elle-même. Dans les offices de plus grande taille ou présentant des risques de sécurité importants, par contre, il est préférable d'engager une ou un CS spécifique à l'office.

La CNT devra notamment délimiter les tâches des CS DIR et celles des CS Office, afin d'éviter une situation malencontreuse où tous deux feraient la même chose, ce qui entraînerait des doublons et des frictions. Il est judicieux que certaines tâches soient accomplies au niveau de l'office et contrôlées au niveau de la Direction, tandis que d'autres ne pourront être accomplies qu'au niveau de cette dernière, le cas échéant avec le soutien des CS Office. Vu les différences de structure et d'organisation TIC des unités administratives des Directions, il est possible que cette répartition ne puisse pas être identique partout.

Lettre *b* : cette formulation tient compte du fait que la même personne doit pouvoir exercer la fonction de CS pour plusieurs unités administratives, pour autant que toutes ces dernières y consentent.

Alinéa 3 :

Les CS accomplissent notamment les tâches suivantes :

a) ils préparent des bases décisionnelles à l'intention de la ou du RS et soumettent des mesures de protection à sa décision ;
b) ils agissent en qualité d'interlocuteurs principaux de leur unité administrative pour les questions relatives à la sécurité de l'information et des données, et conseillent et soutiennent les personnes et services compétents dans l'accomplissement de leurs tâches et l'exécution de leurs obligations ;
c) ils veillent à la mise en œuvre des prescriptions relatives à la sécurité de l'information et des données et au respect de la procédure de sécurité applicable aux outils TIC ;
d) ils surveillent l'inventaire des objets à protéger et la liste des dérogations octroyées ;
e) ils surveillent la planification et la réalisation des mesures de formation et de sensibilisation ;
f) ils coordonnent la gestion des incidents de sécurité et le traitement des vulnérabilités au sein de leur unité administrative et auprès des tiers mandatés ;
g) ils établissent le plan annuel d'audits et de contrôles et le soumettent à l'approbation de la ou du RS ;
h) ils contrôlent périodiquement les outils TIC des catégories « protection élevée » ou « protection très élevée » qui sont en place dans leur domaine de compétence et, le cas échéant, leur sécurité ;
i) sur mandat de la ou du RS, ils contrôlent ou font contrôler comment sont utilisées les informations et données personnelles dans les outils TIC et les espaces de travail ouverts, partagés ou non verrouillables de l'unité administrative ;
j) les CS DIR rendent compte chaque année à la ou au RS DIR de la mise en œuvre et de l'efficacité de la sécurité de l'information ;
k) ils coordonnent la gestion des risques dans le SMSI de leur unité administrative ;
l) ils collectent les indicateurs de leurs unités administratives et veillent à ce que les rapports sur le SMSI soient présentés conformément aux directives du groupe spécialisé SID ;
m) ils assurent l'encadrement des CS Office dans leur domaine de compétence.

Alinéa 4 :

N'appelle aucun commentaire.

Article 38 – Groupe spécialisé Sécurité de l'information et des données

Le groupe spécialisé Sécurité de l'information et des données (SID) existe déjà sous le nom « groupe spécialisé Sécurité de l'information (SI) ». Cet article en précise la composition et les tâches. Pour le statut et les tâches des groupes spécialisés en général, voir l'article 19 OAN.

Principalement chargé de coordonner la sécurité de l'information au niveau interdirectionnel, le groupe spécialisé SID édicte les directives relatives à la présentation des rapports sur le SMSI.

Article 39 – Service de conseil en sécurité de l'information et des données

Alinéa 1 :

Le service de conseil SID correspond à l'actuel domaine spécialisé Sécurité de l'OIO, qui regroupe plusieurs conseillères et conseillers en sécurité appuyant la réalisation des projets TIC de l'administration cantonale. Par rapport à l'actuel domaine, il s'occupera en plus de la conception, de l'exploitation et de la coordination du SMSI cantonal. Il n'exercera pas de fonction de contrôle et de surveillance pour deux raisons : premièrement la responsabilité en matière de sécurité incombe aux RS ou aux organes de direction et, deuxièmement, la surveillance du respect des prescriptions SID relève de la compétence de l'autorité de protection des données et du Contrôle des finances, deux entités indépendantes de l'administration.

Le service de conseil SID accomplit notamment les tâches suivantes :

a) il élabore la stratégie et les objectifs en matière de sécurité de l'information ainsi que les dispositions d'exécution relatives à la sécurité de l'information et des données à l'intention de la CNT ;
b) il tient et met à jour une liste des prescriptions pertinentes pour la sécurité de l'information et des données ;
c) lorsqu'un projet d'une unité administrative est important pour la sécurité, il peut exiger des informations, prendre position sur le sujet et demander des modifications aux RS ;
d) il participe à la formation des organes de l'organisation de sécurité ;
e) il fournit les modèles et outils déclarés contraignants par la CNT ;
f) il conseille et soutient les RS et les CS ;
g) il représente le canton au sein des organisations spécialisées dans la sécurité de l'information et est l'interlocuteur de la Confédération pour les questions relatives à la sécurité de l'information (art. 86, al. 3 LSI) ;
h) en collaboration avec la police cantonale, il peut conclure avec la Confédération, au nom du canton, une convention de prestations sur le contrôle élargi (art. 35 de l'ordonnance de la Confédération du 8 novembre 2023 sur les contrôles de sécurité relatifs aux personnes, OCSP[32]) ;
i) en collaboration avec le groupe spécialisé SID, il conçoit, exploite et coordonne le SMSI et veille à ce qu'il soit contrôlé et efficace.

Ces offres ne sont en principe disponibles que pour les autorités cantonales. Les seules prestations que le conseil SID propose aux autres autorités sont des formations initiales et continues, fournies contre rémunération (art. 19, al. 2 LSIC). L'OIO et le BPD ont donc convenu de se répartir les tâches comme suit :

a) l'autorité cantonale de protection des données élabore, en coordination avec le service de conseil SID, des modèles de documents et des outils conçus dans le cadre de ses conseils aux autorités communales ;
b) le service de conseil SID prépare l'essentiel de ses modèles de document et de ses outils à l'intention des autorités cantonales et de celles qui entendent garantir la protection de leurs propres informations classifiées.

Alinéas 2 et 3 :

N'appellent aucun commentaire.

[32] OCSP, RS 128.31

Article 40 – Récompense pour la découverte et la communication de vulnérabilités

Alinéas 1 et 2 :

Ces dispositions décrivent le programme de primes aux bogues (*Bug Bounty Program*), un dispositif créé par des entreprises ou des autorités pour récompenser des spécialistes en sécurité (*bug hunters*) qui détectent des vulnérabilités (bugs) dans des outils TIC et les communiquent aux personnes responsables. Le processus se déroule généralement comme suit :

1. L'autorité cantonale détermine l'outil TIC à examiner, l'étendue de l'analyse (*scope*) et les règles à respecter, par exemple l'interdiction d'attaquer le DoS ou d'accéder aux données de la clientèle.
2. Les personnes qui y participent ciblent leurs recherches sur les vulnérabilités correspondant à ce *scope* et aux règles définies.
3. Les vulnérabilités repérées sont communiquées via une plateforme de primes aux bogues.
4. L'autorité évalue les informations reçues, confirme et corrige la vulnérabilité identifiée, puis verse le cas échéant une prime (*bounty*) calculée en fonction du risque de sécurité et des règles convenues.

Les programmes de primes aux bogues constituent actuellement un « système de pointe » pour identifier et corriger les vulnérabilités de manière préventive. Plusieurs autorités et entreprises suisses les utilisent, par exemple la Poste Suisse SA, Abraxas Informatique SA, l'Office fédéral de la cybersécurité (OFCS) ainsi que les cantons de St-Gall, Zurich, Thurgovie et Argovie. Il est prévu de recourir aux services d'un fournisseur de plateformes de primes aux bogues professionnel.

Alinéa 3 :

Sur le site Internet correspondant, le service de conseil SID précisera les règles du programme, en soulignant notamment qu'aucune récompense ne sera versée au personnel ni aux mandataires du canton, car la transmission d'informations sur les vulnérabilités fait partie de leurs obligations. Le plafond fixé par le canton de Berne correspond approximativement à celui de la Poste, qui prévoit 10 000 euros pour la communication des vulnérabilités les plus graves.

Alinéa 4 :

L'exclusion de tout droit à une récompense évite les recours relatifs au versement d'une prime ou à sa valeur. Elle se justifie par le fait que les montants en jeu sont faibles, que l'évaluation du droit à une récompense requiert des connaissances poussées en matière de sécurité et est donc difficile à juger, et que l'expérience démontre que la plupart des signalements de vulnérabilités viennent de l'étranger, ce qui compliquerait encore les procédures de recours.

7.5 Dispositions transitoires et finales

Art. 41 – Dispositions transitoires

Alinéa 1 :

Le SMSI est opérationnel depuis le 1er janvier 2025, avec tous les processus correspondants, sauf celui de gestion des risques en matière de sécurité de l'information, qui fait l'objet de travaux depuis le déploiement du SMSI. Les unités administratives y ont intégré leurs quelque 1 400 applications. Vu la progression rapide de la mise en œuvre, les deux ans prévus sont appropriés.

Alinéa 2 :

Les applications cantonales répertoriées dans l'ITSMS indiquent d'ores et déjà les besoins de protection identifiés et, partant, les niveaux de protection requis. L'inventaire des objets à protéger est donc disponible. Au-delà d'être un outil simple et efficace pour le personnel, le catalogue de classification constitue un précieux instrument de pilotage pour assurer une classification uniforme, et surtout économique, à l'échelle de l'administration. L'OIO prévoit d'élaborer un modèle à cet effet. Dans ce contexte, le délai d'un an est raisonnable.

Alinéa 3 :

Les autorités cantonales et leur personnel sont tenus de vérifier dans quels cas il est judicieux d'imposer cette classification a posteriori ainsi que l'apposition de sa mention au moyen de l'outil TIC.

Alinéa 4 :

Lettre *a* : les analyses des besoins de protection et les concepts SIPD se sont certes systématisés au cours des dernières années. Pourtant, ils n'existent pas encore pour tous les outils TIC de l'administration cantonale, alors même que l'établissement de ces documents est obligatoire depuis l'entrée en force de l'OD SIPD, le 1er avril 2011. Cette obligation figure aussi dans l'IPSIC, en vigueur depuis le 1er janvier 2025. Dans ce contexte, les délais d'un an pour l'analyse des besoins de protection et de deux ans pour le concept SIPD sont raisonnables.

Lettre *b* : en vertu de l'article 8 OSID, les autres autorités, et en particulier les autorités et collectivités communales, doivent réaliser une analyse des besoins de protection et un concept SIPD pour leurs fichiers de données personnelles en tenant compte des risques identifiés. Bien que cette obligation existe déjà, la manière dont les autorités de surveillance communales vérifient son application varie d'un cas à l'autre, raison pour laquelle le besoin de rattrapage devrait être plus important. Afin de soulager tant les autorités assujetties que l'autorité cantonale de protection des données, les délais prévus sont de deux ans pour l'analyse et de trois ans pour le concept.

Alinéa 5 :

Les analyses des besoins de protection et les concepts SIPD ne suffisent pas à assurer la protection effective. Celle-ci suppose aussi et surtout que les fabricants et les exploitants d'outils TIC fournissent des prestations sûres conformes aux dispositions contractuelles. Les contrats et outils TIC existants devront donc être adaptés aux prescriptions de l'OSID dès leur prochaine modification. Le délai du 1er octobre 2030 correspond à la disposition transitoire figurant à l'article 16 OCPD, intitulé « Contrats en cours avec des tiers mandatés », selon lequel les contrats doivent être adaptés aux conditions de l'article 1 OCPD dans le délai imparti.

Alinéa 6 :

Il n'est pas dans l'intérêt des communes que les contrôles préalables soumis à l'autorité de surveillance communale soient transférés à l'autorité cantonale de protection des données, qui devrait alors reprendre les dossiers à zéro. Cette disposition transitoire vise à éviter de retarder la mise en œuvre des projets de numérisation communaux.

Alinéa 7 :

Depuis l'entrée en vigueur de l'ordonnance sur la classification, la publication et l'archivage des documents relatifs aux affaires du Conseil-exécutif (OCACE), en 2013, la classification des affaires du Conseil-exécutif fait l'objet d'une réglementation spécifique. En sa qualité de *lex specialis* en la matière, l'OCACE reste applicable aux affaires du Conseil-exécutif et à leurs documents malgré la LSIC, mais sera révisée et adaptée après l'adoption de la nouvelle législation sur la sécurité de l'information et des données.

Article 42 – Modification d'actes législatifs

Lettre *a* : Ordonnance sur l'administration numérique (OAN)

Article 9 – Procédures d'identification

Alinéa 2 : cet alinéa est abrogé. Son objet, à savoir des prescriptions de sécurité, et plus précisément des mesures permettant d'authentifier les utilisatrices et utilisateurs de prestations numériques en tenant compte des risques, relève du champ d'application de l'OSID. Il doit donc être retiré de l'OAN. Vu son niveau de détail, la disposition ne sera cependant pas reprise telle quelle dans l'OSID, mais développée dans une instruction dans laquelle elle sera probablement mise à jour, puisque le standard eCH, relativement abstrait, qui était jusqu'ici la norme de référence pour la qualité du service de connexion cantonal BE-Login, est remplacé par le système d'authentification (AGOVaq), du service de connexion national AGOV. Ce déplacement du contenu de cet alinéa dans l'arsenal réglementaire cantonal sur la sécurité montre aussi clairement que, comme pour les autres mesures de sécurité, les RS peuvent accorder des dérogations lorsqu'ils acceptent expressément le risque qui en découle.

Article 18 – Conférence pour l'administration numérique et les TIC (CNT)

Alinéa 1 :

- les Services parlementaires sont ajoutés à la lettre *c* ;
- l'alinéa est complété par la lettre *e*, qui précise que la ou le CS CNT est également membre de la CNT.

Alinéa 2 : en vertu de la lettre *c*, la CNT dispose désormais aussi de la compétence d'édicter des instructions relatives à la sécurité de l'information et des données.

Article 19 - Groupes spécialisés

Alinéa 2 : sur proposition des Services parlementaires, la lettre *d* est abrogée.

Lettre *b* : Ordonnance sur la Caisse de compensation du canton de Berne et ses agences (OCCB)[33]

[33] OCCB, RSB 841.111

Article 6 - Avec l'Intendance cantonale des impôts

Alinéa 3 : la journalisation des accès aux données ne repose plus sur les dispositions de l'OPD, mais sur celles de l'OSID.

Lettre *c* : Ordonnance sur le traitement des données dans le domaine de l'asile, des réfugiés et des étrangers (ODARE)[34]

Article 9, alinéa 1 (version en vigueur jusqu'au 31 août 2026) : « mesures techniques et organisationnelles » au sens de l'OPD est remplacé par « mesures de sécurité » au sens de l'OSID, et « Bureau cantonal pour la surveillance de la protection des données » par « autorité cantonale de protection des données ».

Article 43 – Abrogation d'un acte législatif

Ordonnance de Direction concernant la sûreté de l'information et la protection des données (OD SIPD)

L'OD SIPD est abrogée, car son contenu est désormais repris dans l'OSID.

Article 44 – Entrée en vigueur

L'OCPD est déjà entrée en vigueur le 1er septembre 2026, soit à la même date que la LCPD, tandis que l'OSID ne prendra effet que le 1er novembre 2026, en même temps que la LSIC. Cette entrée en vigueur à une date ultérieure s'explique par le fait que l'OSID a fait l'objet d'un second corapport après qu'elle a été entièrement remaniée pour faciliter sa compréhension. S'agissant du délai transitoire, l'article 18 OCPD déclare applicables les articles 4 à 9 OPD (« Mesures techniques et organisationnelles » et « Contrôle préalable »), qui seront notamment remplacés par les articles 5 à 10 OSID à compter du 1er novembre 2026.

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

L'OSID s'inscrit dans le programme gouvernemental de législature 2023 à 2026, qui prévoit, comme deuxième objectif, que le canton de Berne exploite la transformation numérique pour fournir des services de haute qualité, efficaces et efficients. La qualité de ces services implique qu'ils soient sécurisés, une condition essentielle pour que la population et les acteurs économiques soient disposés à confier leurs données personnelles et leurs informations à caractère confidentiel aux autorités.

Elle correspond aussi à la stratégie Administration numérique et TIC : Stratégie 2026-2030 arrêtée par le Conseil-exécutif le 11 juin 2026, qui, au chiffre 6.5, fait de la sécurité de l'information un principe stratégique.

[34] DAFAV, BSG 861.112

9. Répercussions sur les finances, l'organisation, le personnel, l'informatique et les locaux

9.1 Sécurité de l'information

Pour ce qui est des répercussions financières, nous pouvons reprendre ici le contenu du rapport sur la LSIC (ch. 10 et 11) :

Les mesures de protection visant à garantir la sécurité de l'information doivent en principe être mises en œuvre avec les moyens financiers existants et planifiés dédiés aux s TIC et à la numérisation. Et ce pour les raisons suivantes :

a) L'article 17 de la LCPD en vigueur à ce jour oblige d'ores et déjà les autorités à garantir la sécurité des données. La LSIC n'instaure donc pas de nouvelle tâche étatique, mais elle concrétise seulement une tâche existante.

b) La numérisation de l'administration est certes un inducteur de coûts en matière de TIC et donc de sécurité de l'information et de cybersécurité, particulièrement dans le contexte des menaces croissantes qui pèsent sur la cybersécurité. Toutefois, la LAN et la LSIC mettent dans les mains des autorités responsables plusieurs outils qui leur permettent de réduire ou de compenser ces surcoûts :

    1. Si les autorités automatisent davantage leurs échanges avec les entreprises et les professionnels (voir art. 8 LAN) et dématérialisent comme il se doit les processus, elles peuvent réduire leurs coûts de matériel et de personnel (pour le traitement des dossiers, le secrétariat, la saisie des données, le port, le papier, l'impression, etc.).

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

    3. Si les autorités appliquent une gestion des risques appropriée (art. 5, al. 2 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. 12, al. 1, lit. d LSIC). Si elles se bornent à classifier uniquement les informations nécessaires (art. 8, al. 3 LSIC), elles réduisent le nombre de systèmes à catégorie de sécurité élevé (art. 12, al. 2, lit. b LSIC) et, par conséquent, les coûts qui en résultent.

Les répercussions sur le personnel seront également restreintes au minimum du fait que les organes spécialisés dans la sécurité de l'information seront intégrés à l'actuelle gouvernance de l'administration numérique et des TIC.

Dans l'hypothèse où des programmes de primes aux bogues seraient lancés, leurs coûts seront inscrits au budget de l'OIO (env. CHF 40 000 par an pour la plateforme, env. CHF 60 000 par an pour les primes). Les coûts réels dépendent du nombre de communications. Les charges de personnel d'environ 0,25 EPT seront compensées au sein de l'OIO.

La formation du personnel via BE-Secure continuera d'être proposée par l'OIO. Elle ne durera pas plus de deux heures. De même, les campagnes de sensibilisation à l'échelle de l'administration seront comme auparavant lancées et financées par l'OIO.

Le rôle de la ou du CS CNT sera assumé par la personne à la tête du service de conseil SID rattaché à l'OIO, soit l'actuel organe spécialisé Sécurité de l'OIO. Aucune autre création de poste n'est prévue.

Les DIR/CHA/JUS comptent déjà un ou une RS, mais son statut hiérarchique, sa formation et son pourcentage de poste diffèrent fortement d'un service à l'autre. La haute direction devra procéder à un état des lieux et apporter les changements nécessaires.

Un audit coûte environ 20 000 francs. Il est d'ores et déjà possible de faire appel à des spécialistes externes pour réaliser ces audits en utilisant les contrats-cadres mis à disposition par l'OIO. La coordination entre les DIR/CHA/JUS ainsi qu'avec le Contrôle des finances et le Bureau pour la protection des données doit permettre de réduire le nombre d'audits au strict minimum compte tenu des risques.

La conception et l'exploitation de la plateforme centralisée de signalement relève de la compétence de l'OIO, qui prévoit des charges annuelles d'environ 5000 francs.

En résumé, il est impossible pour l'instant d'établir des prévisions fiables sur les ressources en personnel nécessaires pour les nouveaux instruments à mettre en place (SMSI, inventaire des objets à protéger, audits). Il n'est donc pas exclu que, dans le cadre des futurs processus de planification, les Directions et la Chancellerie d'État présentent des besoins en ressources supplémentaires.

9.2 Sécurité des données

Avec la révision de la LCPD et le traitement informatisé de données personnelles et du profilage à risque élevé inscrit dans son article 2, lettre *h*, les exigences en matière de sécurité des données se durcissent.

Dans cet esprit, l'article 6, alinéa 2 OSID prévoit que, lorsque les mesures de prévention ne suffisent pas à garantir la sécurité des données, la lecture et la communication de données personnelles sensibles soient ajoutées à la liste actuelle des éléments à journaliser que sont l'enregistrement, la modification, l'effacement et la destruction.

L'obligation de journaliser existe déjà depuis 2008 à l'article 5, alinéa 1, lettre *h* OPD BE. Les procédures visant à garantir la sécurité des données, désormais expressément définies dans l'OSID, permettront néanmoins de détecter et de sécuriser les outils TIC jusqu'ici exploités illicitement en l'absence de journalisation, ce qui générera des coûts qui auraient déjà dû être engagés à la mise en service de ces outils.

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

10.1 Sécurité de l'information

La LSIC ne s'applique aux communes et aux autres organisations chargées de tâches publiques 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). Dans ce contexte, elles doivent respecter les règles régissant la classification et le maniement des informations classifiées et des systèmes TIC.

Elles 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.

10.2 Sécurité des données

L'OSID régissant aussi bien la sécurité de l'information que des données, elle s'applique en vertu de la LCPD à toutes les autorités qui traitent des données personnelles (voir art. 2, al. 2, lit. *c* OSID). Comme exposé ci-après, la sécurité des données n'est cependant pas une nouveauté, ni pour les autorités cantonales ni pour les autres autorités. L'OSID ne fait que concrétiser des tâches existantes, sans en créer de nouvelle. La complexité croissante de l'accomplissement de ces tâches ne découle pas de la législation, mais de l'extension de la numérisation de l'administration publique et de la multiplication des cyberrisques qui en résulte.

Depuis qu'elle a été édictée, en 1986, la LCPD exige à l'article 17 que la sécurité des données soit garantie, une prescription que les articles 4 et 5 OPD (Mesures techniques et organisationnelles) ont précisée. Les articles 5 et 6 OSID reprennent ces dispositions en les actualisant. L'obligation d'effectuer des contrôles préalables lors du traitement de données au moyen d'outils TIC existe elle aussi depuis longtemps déjà (1986 également) à l'article 17a LCPD.

La sécurité des données a encore été concrétisée en 2011 dans l'OD SIPD, en particulier en ce qui concerne la procédure de sécurité applicable aux outils TIC et l'organisation de la sécurité, pour cette dernière toutefois uniquement en lien avec l'administration cantonale.

En vertu de l'OSID, les principes de la sécurité de l'information et des données ainsi que des organes de direction visés à l'article 4 OSID valent pour l'ensemble des autorités du canton de Berne, y compris pour les communes municipales, les paroisses et les communes bourgeoises. Par contre, les articles 13 et suivants OSID ne visent que les autorités cantonales ; les prescriptions relatives au SMSI, à l'inventaire des objets à protéger, aux contrôles et aux audits, ou à la classification des informations, notamment, ne concernent pas les autres autorités.

11. Répercussions sur l'économie

L'évaluation de la LSIC réalisée à l'aide de la check-list pour l'analyse d'impact de la réglementation a déjà 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.

La participation active de spécialistes de Bedag Informatique SA, Swisscom SA et SPIE Suisse SA à l'élaboration de l'OSID n'a pas modifié les résultats obtenus.

Ce constat a encore été confirmé par les travaux sur la protection de base BE menés parallèlement à l'édiction de la présente ordonnance. En plus des trois entreprises précitées, les deux principaux prestataires externes des communes municipales bernoises, Dialog Verwaltungsdata SA et Talus SA, ont été associés à la consultation sur les mesures de sécurité concrètes. Ni l'un ni l'autre ne craignent de coûts supplémentaires ou d'autres conséquences négatives sur leur activité, car leurs mesures de sécurité se fondent déjà sur la norme ISO-27001.

12. Proposition

La Direction des finances propose au Conseil-exécutif d’édicter la présente ordonnance.

Annexe
– Projet d’acte législatif