



Intervention parlementaire

Réponse du Conseil-exécutif

N° de l'intervention : 308-2025
Type d'intervention : Interpellation
Motion ayant valeur de directive : ☐
N° d'affaire : 2025.GRPARL.1484

Déposée le : 24.11.2025

Motion de groupe : Non
Intervention de l'organe du GC : Non
Déposée par : Daphinoff (Bern, Le Centre) (porte-parole)
Roggli (Rüschegg Heubach, Le Centre)
Rappa (Burgdorf, Le Centre)
Gerber (Schüpfen, Le Centre)

Cosignataires : 0

Urgence demandée : Non
Urgence accordée :

N° d'ACE : 621/2026 du 3 juin 2026
Direction : Chancellerie d'État
Classification : Non classifié

Cybersécurité et intégrité des élections dans le canton de Berne

Ces dernières années, la numérisation croissante a joué un rôle grandissant dans le déroulement des élections et des votations dans le canton de Berne. Si ces développements améliorent l'efficacité et l'accès aux informations électorales, ils posent également de nouveaux défis, notamment en matière de cybersécurité.

En ces temps de cybermenaces croissantes, la sécurité des élections et des votations revêt une très haute importance. Le canton de Berne doit s'assurer que tous les processus électoraux – de la collecte des suffrages à la publication des résultats – sont protégés des attaques, des manipulations et de la désinformation. Un système électoral transparent, sûr et équitable est en effet indispensable pour perpétuer la confiance de la population dans les institutions démocratiques.

Compte tenu de la numérisation croissante de l'infrastructure électorale et de l'augmentation des menaces de cyberattaques et de campagnes de désinformation numériques, il est essentiel que le canton de Berne prenne des mesures proactives afin d'assurer la sécurité des processus électoraux et de garantir la protection des données des électrices et électeurs. Dans ce contexte, la question se pose de savoir dans quelle mesure le canton de Berne est préparé à faire face aux risques croissants de cyberattaques et de manipulations numériques.

Le Conseil-exécutif est prié de répondre aux questions suivantes :

1. Quels sont les moyens mis en œuvre pour assurer la sécurité de l'infrastructure numérique utilisée pour la collecte et la transmission des résultats électoraux ? Quelles sont les mesures concrètes qui ont été mises en œuvre jusqu'à présent pour préserver la sécurité

de cette infrastructure contre le piratage ou pour faire front contre toute autre intervention non autorisée ?

2. Dans quelle mesure la protection des données électorales sensibles (p. ex. données des électrices et électeurs, bulletins de vote, résultats des élections) est-elle assurée au niveau cantonal et communal ? Quelles sont les mesures techniques et organisationnelles mises en place pour protéger ces données contre tout accès non autorisé, toute perte ou tout abus ?
3. Quels moyens le canton met-il en œuvre pour s'assurer que les élections et les votations soient protégées contre les campagnes de désinformation numérique et les influences ciblées (p. ex. dues aux fausses nouvelles ou à la manipulation à travers les réseaux sociaux) ? Quelles sont les mesures prises pour maintenir la confiance de la population dans l'intégrité des processus électoraux ?
4. Quels sont les moyens mis en œuvre pour sensibiliser et former les personnels des administrations communales et des bureaux électoraux en ce qui concerne les risques liés à la cybersécurité dans le contexte des élections et des votations ? Le canton propose-t-il aux communes un point de contact centralisé ou un soutien pour répondre à leurs éventuelles questions en lien avec la sécurité informatique au niveau du processus électoral ?
5. Dans quelle mesure le canton de Berne coopère-t-il avec d'autres institutions, telles que le Centre national pour la cybersécurité (NCSC), la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), d'autres cantons ou les hautes écoles spécialisées (p. ex. HESB, EPFL), afin de renforcer la cybersécurité des processus électoraux ? Des coopérations concrètes ou des initiatives communes ont-elles été mises sur pied pour améliorer la sécurité des élections et des votations ?

Réponse du Conseil-exécutif

Depuis 2018, le canton de Berne utilise le logiciel BEWAS pour dépouiller les scrutins fédéraux, cantonaux et régionaux et en publier les résultats. BEWAS est une application en ligne de la société Bedag Informatique SA. La Bedag a développé le logiciel et fournit au canton de Berne des prestations d'entretien, de maintenance, d'exploitation et d'assistance. Les bases légales du recours à une application informatique pour déterminer les résultats des votations et des élections reposent sur l'article 53, alinéa 1 de la loi sur les droits politiques (LDP). BEWAS est doté d'un concept de sécurité de l'information et de protection des données (concept SIPD) qui recense et évalue les risques en matière de protection des données et de sécurité.

Le Conseil-exécutif répond comme suit aux questions posées :

1. *Quels sont les moyens mis en œuvre pour assurer la sécurité de l'infrastructure numérique utilisée pour la collecte et la transmission des résultats électoraux ? Quelles sont les mesures concrètes qui ont été mises en œuvre jusqu'à présent pour préserver la sécurité de cette infrastructure contre le piratage ou pour faire front contre toute autre intervention non autorisée ?*

L'instruction sur la protection de base en matière de sécurité de l'information et de cybersécurité (IPSIC) définit les exigences en matière de protection de base pour les ressources TIC, les informations ainsi que les données personnelles des autorités

cantoniales. Le concept SIPD décrit les mesures supplémentaires prises pour réduire les risques à un niveau acceptable.

L'infrastructure de la Bedag respecte pleinement ces prescriptions. En outre, la Bedag exploite un système de management de la sécurité de l'information (SMSI) certifié selon la norme ISO 27001:2022, un système de management de la continuité d'activité certifié selon la norme ISO 22301:2019 ainsi qu'un système de gestion des services certifié selon la norme ISO 20000:2018. Il existe par ailleurs des systèmes certifiés de management environnemental (ISO 14001:2015) et de management de la qualité (ISO 9001:2015).

De plus, la Bedag a mis en place un programme complet de test de sécurité, dans lequel BEWAS est également contrôlé régulièrement par des entreprises externes et indépendantes. Les éventuelles mesures d'amélioration et de correction prennent systématiquement en compte les résultats de ces tests.

2. *Dans quelle mesure la protection des données électorales sensibles (p. ex. données des électrices et électeurs, bulletins de vote, résultats des élections) est-elle assurée au niveau cantonal et communal ? Quelles sont les mesures techniques et organisationnelles mises en place pour protéger ces données contre tout accès non autorisé, toute perte ou tout abus ?*

Il convient avant toute chose de préciser qu'aucune donnée particulièrement digne de protection n'est traitée dans BEWAS. Comme la carte de légitimation est séparée du bulletin de vote ou du bulletin électoral avant le dépouillement, le secret du vote est garanti en tout temps. Les bulletins de vote et les bulletins électoraux sont décomptés au sein des communes sans l'assistance technique du canton. Les communes peuvent recourir à leur propre outil de décompte des voix (p. ex. logiciel de dépouillement). Les bureaux électoraux ne saisissent dans BEWAS que les résultats communaux décomptés, que la Chancellerie d'État publie ensuite sur Internet. Les bureaux électoraux peuvent comparer en tout temps les résultats communaux publiés par le canton avec les procès-verbaux communaux.

Les aspects sécuritaires revêtent une importance majeure lors du recours à des technologies numériques. Comme évoqué en introduction, BEWAS est doté d'un concept SIPD. Le personnel des communes, des préfectures et de la Chancellerie d'État doit passer par une authentification à deux facteurs pour accéder au logiciel. Les utilisatrices et utilisateurs doivent se connecter au moyen d'une adresse électronique saisie au préalable par le service compétent (préfectures ou CHA) ainsi que d'un mot de passe et d'un code à usage unique. Avant chaque scrutin, la Chancellerie d'État et les préfectures mettent à jour la liste des utilisatrices et utilisateurs. Toutes les manipulations effectuées dans le système sont consignées au moyen d'un journal d'audit. De même, l'ensemble des activités en lien avec la connexion et le compte sont enregistrées.

BEWAS est disponible en ligne et son exploitation est assurée par le centre de calcul de la Bedag. Il n'existe aucune interface directe avec d'autres réseaux. Les capacités de calcul sont dupliquées dans des locaux techniques jumeaux et cloisonnés. Elles sont configurées de façon à offrir, aussi bien au niveau du système que de l'application, une sécurité aussi élevée que possible en cas de dérangement, et à garantir l'évolutivité. Quotidienne et entièrement automatisée, la sauvegarde des données se fait dans le centre de calcul Data Safe de la Bedag, au Noirmont. De plus, il existe une stratégie en cas d'urgence et une convention de service qui garantissent une assistance individuelle de premier ordre par le personnel de la Bedag les jours de scrutin.

3. *Quels moyens le canton met-il en œuvre pour s'assurer que les élections et les votations soient protégées contre les campagnes de désinformation numérique et les influences ciblées (p. ex. dues aux fausses nouvelles ou à la manipulation à travers les réseaux sociaux) ? Quelles sont les mesures prises pour maintenir la confiance de la population dans l'intégrité des processus électoraux ?*

La désinformation est la diffusion intentionnelle de fausses informations en vue de tromper la société, des groupes ou des individus à des fins politiques ou économiques¹. Les campagnes de désinformation ne se limitent pas au canton de Berne. La Suisse entière est confrontée à de possibles activités d'influence, notamment par le truchement de la désinformation.

Dans le contexte de tensions géopolitiques en hausse, il faut s'attendre à une recrudescence de ce type d'activités en Suisse également. Le Conseil fédéral a donc instauré, le 26 novembre 2025, un groupe de travail interdépartemental contre les activités d'influence et la désinformation (GTID)². Son objectif est de renforcer les travaux menés au sein de l'administration fédérale en lien avec les activités d'influence et la désinformation, de dresser un état des lieux de la situation et, si nécessaire, de proposer des mesures aux décideuses et décideurs politiques. Le GTID est dirigé par le Secrétariat d'État à la politique de sécurité (SEPOS) et regroupe les offices les plus concernés par la menace. La Chancellerie fédérale, compétente en matière de droits politiques, en fait notamment partie. La Chancellerie d'État est en contact avec la Chancellerie fédérale à ce sujet.

Le Conseil-exécutif salue la démarche de la Confédération. En effet, face aux activités d'influence d'ampleur internationale, il est judicieux que la Confédération s'empare de la thématique. Le canton s'efforce, dans sa propre communication publique, de susciter la confiance. Il exploite ses canaux de communication officiels pour informer de façon proactive, transparente, franche et crédible sur les élections et les votations. Avant, pendant et après chaque scrutin, le public obtient des informations actuelles par le biais de communiqués de presse, de publications sur les réseaux sociaux, de l'application VoteInfo, de la Feuille officielle ainsi que du site Internet du canton.

Le déroulement des élections et votations ainsi que les responsabilités sont régis par la loi. Le dépouillement se déroule en public et le double contrôle s'applique au bureau électoral pour toutes les démarches pertinentes. Toute personne peut dénoncer au Conseil-exécutif des irrégularités ou des vices survenus lors d'une votation ou d'une élection, ou en rapport avec une demande de vote populaire ou une initiative populaire.

4. *Quels sont les moyens mis en œuvre pour sensibiliser et former les personnels des administrations communales et des bureaux électoraux en ce qui concerne les risques liés à la cybersécurité dans le contexte des élections et des votations ? Le canton propose-t-il aux communes un point de contact centralisé ou un soutien pour répondre à leurs éventuelles questions en lien avec la sécurité informatique au niveau du processus électoral ?*

Avant chaque élection selon le mode proportionnel, les communes sont tenues de tester les processus techniques à mettre en œuvre le jour du scrutin. Lors d'élections selon le mode majoritaire ou lors de votations, ce test est facultatif. Les communes peuvent s'aider des listes de contrôle détaillées mises à leur disposition. En cas de question, elles doivent tout

¹ Source : glossaire du DFAE -> Désinformation

² <https://www.admin.ch/fr/newsb/PhlsbTXMF5o3YiuqfGumj>

d'abord s'adresser à leur préfecture. Si nécessaire, la Chancellerie d'État ou la Bedag apportent leur assistance.

5. *Dans quelle mesure le canton de Berne coopère-t-il avec d'autres institutions, telles que le Centre national pour la cybersécurité (NCSC), la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), d'autres cantons ou les hautes écoles spécialisées (p. ex. HESB, EPFL), afin de renforcer la cybersécurité des processus électoraux ? Des coopérations concrètes ou des initiatives communes ont-elles été mises sur pied pour améliorer la sécurité des élections et des votations ?*

La Bedag échange régulièrement à plusieurs niveaux avec des institutions fédérales et internationales afin de renforcer sa cybersécurité. Elle collabore aussi étroitement avec l'Office fédéral de la cybersécurité (OFCS).

Le Conseil-exécutif est favorable sur le fond à d'autres étapes de numérisation dans le domaine des droits politiques. Au vu des risques actuels, il est en effet indispensable de fixer des exigences élevées en ce qui concerne la sécurité technique du système en lien avec le vote électronique, ce qui a également des conséquences sur les coûts. Le Conseil-exécutif va donc se pencher attentivement sur les prochaines étapes de numérisation et les examiner d'un œil critique, notamment sous l'angle de la sécurité.

Destinataire
– Grand Conseil