Compte rendu de la réunion du 20 janvier 2022
1ère réunion de sécurité / expertise indépendante

MM. Eric Regazzo et Jérôme Combier présidaient la première réunion de sécurité du système de vote par correspondance sur Internet en présence de M. Bernard Starck, expert indépendant.

L'administration a rappelé tout d'abord le contexte général en évoquant le cadre réglementaire. Il faut en particulier se référer aux décrets 2020-1426 & 2020-1427 du 20 novembre 2020 relatifs au CAP et CSA et au décret 2011-595 relatif au vote électronique, encadré par la délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. Dans le silence des dispositions spécifiques, on se référera généralement au code électoral.

Les trois acteurs principaux sont :

- le MEFR qui avait déjà réussi l'exercice en 2018 ;
- le MEAE qui avait organisé des élections consulaires et législatives par voie électronique mais qui expérimente le dispositif dans le cadre des élections professionnelles ;
- l'AEFE qui découvre ces technologies et qui disposent d'un personnel qui n'est pas toujours francophone, ni anglophone. Toutefois, aux dires de l'administration, un système électronique, riche en icône, est sans doute plus lisible qu'un mécanisme papier.

Il est rappelé que tout électeur peut se faire assister d'un électeur de son choix, appartenant au même établissement.

Le MEFR disposera d'une authentification forte à deux facteurs : ENSAP (bulletin de paye) et courriel professionnel. Le vote sera validé par un code envoyé sur le téléphone portable de l'agent. Une alternative avec France Connect est envisagée. La communication ministérielle devra être répétée au niveau directionnel.

Les collègues du MEAE recevront par voie postale (ou à la main contre signature) leur carte d'électeur. Ils initialiseront leur mot de passe à l'aide d'un jeton reçu par courriel. L'AEFE se reposera sur son système SSO aefe.fr. Les collègues sont invités à activer leur espace Orion permettant d'activer cette fonctionnalité. L'attention est appelée sur les agents en ADL, très nombreux au MEAE et à l'AEFE, qui ne peuvent bénéficier de l'ENSAP.

Le système de vote sera déployé sur quatre tenants de production séparés :

- celle déliée au MEFR :
- celle dédiée aux AAI et EP rattachées au MEFR ;

- celle dédiée au MEAE ;
- celle dédiée à l'AEFE.

Les données seront initialisées à partir de SIRHIUS, SIRH commun au MEFR et au MEAE. La DGFiP utilisera l'application Orchidée RH et les autres directions économiques et financières, CLE. Le référentiel doit contenir, pour le MEFR :

- 150 000 électeurs ;
- 16 000 candidatures et candidats (dont les listes de professions de foi avec les logos) ;
- 2 000 membres des équipes électorales (bureaux de vote et bureaux de vote centralisateurs) ;
- le référentiel des scrutins.

Les réclamations électorales ne pourront être portées via le système (ouvert un mois avant les élections) qu'avant le vote et le scellement des urnes. Pendant et après le vote, l'électeur doit pouvoir constater la prise en compte de son vote.

Aux fins de tests, les élections blanches se dérouleront fin mars. L'attention est demandée pour que la plus grande diversité des populations soit représentée, notamment celles de l'AEFE sous statut d'ADL, pour lesquelles une traduction du site en anglais sera proposée.

Le système de vote électronique devra être homologué par le MEFR, par le MEAE et par l'AEFE. Cependant, il y aura une **commission d'homologation** unique. Au côté de l'administration, se tiendront 6 représentants des fédérations syndicales :

- 3 pour le MEFR (comme en 2018 où la CGC-Finances était représentée) ;
- 2 pour le MEAE ;
- 1 pour l'AEFE.

La **commission de sécurité** est ouverte à toute fédération qui en fait la demande.

Une **cellule de crise** sera constituée sur la base de la commission de sécurité afin, si nécessaire, de relayer aux différents acteurs les incidents et de suivre leur résolution.

Cette délégation des bureaux de vote électroniques doit assurer la bonne compréhension des évènements par des experts (y compris des fédérations syndicales) connaissant les spécificités du système.

Les discussions de ces instances sont couvertes par la discrétion professionnelle aux fins notamment de ne pas révéler à des tiers des éléments de vulnérabilité compromettant le système de vote.

En fin de séance, la CGC-Finances a fait part de son souhait de participer à ces instances.

L’expertise doit être réalisée par un expert indépendant, c’est-à-dire qu’il devra répondre aux critères suivants :

- être un informaticien spécialisé dans la sécurité ;
- ne pas avoir d’intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d’utiliser la solution de vote ;
- posséder une expérience dans l’analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d’au moins deux prestataires différents.

Chacun des experts, réunis par M. Bernard Starck, remplit ces conditions. Les experts du groupement sont intervenus au titre de l'expertise indépendante des élections professionnelles 2018 sur l'ensemble des Ministères ayant engagé un processus de dématérialisation de leurs élections. En 2019-2020: Ministère du Travail (TPE 2021), Ministère de la Santé (URPS 2021), Ministère des Affaires Étrangères (AFE 2021), Ministère des Armées (CFM, CSFM 2021). Nombreux scrutins dans le secteur privé. Ils interviennent sur de nombreux scrutins de la Fonction publique pour la campagne 2022.

Tout responsable de traitement mettant en œuvre un système de vote par correspondance électronique, notamment via Internet, doit faire expertiser sa solution par un expert indépendant. L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes d'électeurs et leur enrôlement et l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

Le but de l'expertise est de garantir la sincérité des opérations électorales :

- secret du vote,
- complète information de l'électeur,
- égalité entre les candidats,
- caractère personnel et libre du vote,
- surveillance effective du scrutin,
- possibilité de contrôle a posteriori par le juge.

La sincérité du scrutin implique, que le résultat de l'élection soit l'exact reflet de la volonté, du corps électoral. Tout manquement aux principes généraux entraînera une remise en cause de la sincérité du scrutin et l'annulation de l'élection. Le bureau de vote est garant du respect des principes généraux du droit électoral pendant le scrutin.

La recommandation CNIL n° 2019-053 du 25 avril 2019 fixe, de façon pragmatique, les objectifs de sécurité que doit atteindre tout dispositif de vote par correspondance électronique, notamment via Internet, en fonction des risques que présente le déroulement du vote. Les réponses apportées par les systèmes à ces objectifs de sécurité doivent ainsi prendre en compte le contexte et les menaces qui pèsent sur le scrutin.

En revanche, Le système entier est évalué point par point par l'expert en fonction des objectifs de sécurité et de la conformité à la recommandation. Il ne s'agit pas de cocher toutes les cases en vert, mais d'aboutir à une évaluation globale de la sécurité du système au regard des menaces, des moyens et motivations des attaquants. Enfin, l'expert n'est pas là pour lever tous les bogues. « L'expertise est garante du bon fonctionnement du dispositif et de la sincérité et de l'intégrité du vote dans son ensemble ».

Quant aux 23 objectifs de sécurité, les entités ont décidé de tous les prendre en compte pour atteindre le niveau maximal de sécurité (n° 3). Les experts pensent que la grille de notation proposée par la CNIL est difficile à utiliser en l'état. Son application conduit à placer la plupart des scrutins au niveau 3. La méthodologie proposée est d'évaluer chacun des objectifs de niveau 3 et de considérer l'apport de chacun des objectifs au regard des menaces et risques identifiés par rapport aux risques couverts par les deux premiers niveaux et de ne retenir que ceux dont la mise en œuvre est soit une obligation légale soit raisonnablement proportionnée aux risques identifiés. De ce fait, on atteindra une sécurité de niveau 2+.

Pour l'authentification, la CNIL recommande d'utiliser

- un identifiant et un mot de passe ;
- ces deux éléments étant transmis par des canaux séparés ;

- et, en complément, une question défi-réponse non triviale (exclusion de la date de naissance ou de tout autre élément facilement décelable).

Par ailleurs, le système de vote devra permettre à l'électeur de vérifier la prise en compte effective de son vote tout au long du scrutin. La solution est à l'étude.

La sécurité d'un scrutin est inversement proportionnelle à la quantité de confiance qu'il est nécessaire d'accorder aux acteurs chargés de le mettre en œuvre. A cette fin, l'expert indépendant accompagnera les équipes de la conception à la mise en production et tout au long des opérations de vote.

La CGC-Finances a rappelé la fiabilité du système déployé en 2018 mais avait toutefois déploré trois incidents majeurs :

- **une plateforme sous-dimensionnée à l'ouverture du scrutin ;**
- **une absence de paramétrage des pastilles (toutes oubliées à l'exception du département de résidence administrative) ;**
- **le blocage d'un dépouillement dans un bureau de vote électronique centralisateur.**

A l'exception des pastilles, tous les incidents avaient été heureusement résolus.

Une deuxième réunion de sécurité est prévue pour le jeudi 3 mars 2022.