CNIL.

Délibération n° 2009-197 du 26 mars 2009 de la formation restreinte prononçant un avertissement à l'encontre du ministre du travail, des relations sociales, de la famille et de la solidarité

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TÜRK ;

Etant aussi présents M. Emmanuel de GIVRY, vice-président délégué, Mme Isabelle FALQUE-PIERROTIN, vice-présidente, Mme Claire DAVAL, M. Sébastien HUYGHE et M. Jean-Marie COTTERET, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 ;

Vu la délibération n° 2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu le rapport de M. Philippe GOSSELIN, commissaire rapporteur, notifié par huissier au ministre le 25 février 2009 ;

Vu les autres pièces du dossier ;

Après avoir entendu, lors de la réunion du 26 mars 2009 :

- M. Philippe GOSSELIN, commissaire, en son rapport ;
- Mme Catherine POZZO DI BORGO, commissaire-adjoint du Gouvernement, en ses observations ;
- M. Jean-Denis COMBREXELLE, directeur général du travail ;
- M. Dominique GUENEAUX, expert pour le compte du ministère ;
- M. Thierry CARDONA, expert-informaticien auprès de la CNIL ;

M. Jean-Denis COMBREXELLE ayant pris la parole en dernier ;

I- Faits et procédure

Conformément à l'article 9 de l'ordonnance du 24 juin 2004 disposant que « *pour le prochain renouvellement du mandat des conseillers prud'hommes, le vote électronique est mis en œuvre, à titre expérimental, dans des conditions et selon les modalités définies par décret en Conseil d'Etat. Les matériels et logiciels devront respecter le secret du vote et la sincérité du scrutin* », ainsi qu'au décret du 23 juillet 2007 relatif à l'expérimentation du vote électronique pour les élections prud'homales de 2008 à Paris, et à son arrêté d'application en date du 21 juillet 2008, le ministère du travail, des relations sociales, de la famille et de la solidarité (ci-après « le ministère ») a organisé du 19 novembre au 26 novembre 2008 un vote par internet pour les électeurs inscrits à Paris. La CNIL s'est prononcée sur les textes relatifs à cette expérimentation par un avis du 9 novembre 2006.

Pour mettre en place ce dispositif de vote électronique, la direction générale du travail a contracté avec les sociétés THALES et ELECTION EUROPE. THALES a joué le rôle d'intégrateur de la solution de vote électronique développée par ELECTION EUROPE en en assurant l'hébergement (mise à disposition des serveurs informatiques sur lesquels est installée la solution de vote) et la maintenance.

En application de la décision n° 2008-138 C du 18 novembre 2008 du président de la Commission nationale de l'informatique et des libertés (ci-après « CNIL » ou « la Commission »), plusieurs contrôles sur place ont eu lieu les 19, 24 et 26 novembre 2008 ainsi que le 3 décembre 2008, afin de vérifier les mesures mises en œuvre pour garantir la sécurité et la sincérité du scrutin.

A) Le contrôle du 19 novembre 2008

Une délégation de la CNIL a procédé à un contrôle sur place, le 19 novembre 2008, jour de l'ouverture du scrutin par internet (le scrutin par internet se déroulait du 19 au 26 novembre 2008 et le scrutin « papier » se déroulait le 3 décembre 2008), dans les locaux de la société THALES situés 9 rue Baudouin à Paris (75), où les membres du bureau de vote électronique étaient présents (président, assesseurs et secrétaire du bureau de vote).

La délégation de la CNIL a constaté, en matière d'identification et d'expertise du logiciel installé, que les codes sources (c'est-à-dire les différents programmes constitutifs du système de vote) n'avaient pas été expertisés dans leur intégralité. Cette information figure d'ailleurs dans l'expertise 10/2008 réalisée sur le dispositif de vote par la société Strat-up à la demande du ministère en novembre 2008 (audit indépendant). La délégation a également constaté l'absence d'identification de la version du logiciel installé et de la version du logiciel expertisé.

En matière de chiffrement du bulletin de vote, la délégation de la Commission a constaté que la liaison entre le terminal de vote et le portail internet du dispositif de vote (serveur web) était sécurisée (protocole https). Le vote de l'électeur était brouillé (procédure « d'obfuscation »[1]) dès son émission et jusqu'à sa prise en compte par le serveur d'applications. Ensuite, le serveur d'applications chiffrait le bulletin de vote puis l'enregistrait dans l'urne.

---

[1] La procédure « d'obfuscation » du bulletin de vote consiste à remplacer le nom du candidat par une chaîne de caractères durant son transport (par exemple : M DUPONT devient « 123gfd… »).

[redacted]

S'agissant du descellement de l'urne, la délégation de la CNIL a constaté qu'une modification du dispositif de vote avait été effectuée le 17 novembre 2008, après la procédure de scellement. Cette modification a nécessité un descellement puis un nouveau scellement du dispositif de vote par les sociétés ELECTION EUROPE et THALES. Cette information ne figure ni dans le journal des opérations de vote (créé le 20 novembre 2008), ni dans le constat d'huissier remis à la Commission et joint au courrier du ministère du 2 janvier 2009.

Enfin, la délégation de la CNIL a constaté que la société Election Europe avait créé une urne permettant de recueillir les bulletins de vote correctement exprimés par les électeurs, mais qui seraient illisibles à la suite d'un dysfonctionnement du système et considérés comme nuls par le dispositif de vote.

B) La modification du système de vote du 21 novembre 2008

La CNIL a été informée que les électeurs utilisant le navigateur Firefox dans ses versions 1.5 et 2.x ne pouvaient pas voter. La liste de la CGT et le bouton « voter » n'étaient pas visibles à l'écran. Cette anomalie était liée à un problème d'affichage.

Après avoir pris attache avec la CNIL, et après la validation par des experts mandatés par le ministère, des équipes de THALES, du ministère et des membres du bureau de vote, le système de vote, en particulier son portail d'accès, a été modifié le 21 novembre 2008 par les sociétés ELECTION EUROPE et THALES. Cette modification a consisté à mettre à jour la page en cause. Cela a été fait en utilisant le compte de connexion « Hamdi bis », détenu par la société THALES, sans procéder au descellement de la plateforme. La procédure suivie a été décrite dans le procès-verbal établi par l'huissier de justice.

C) Les contrôles du 24 novembre 2008

Une délégation de la CNIL a procédé à deux contrôles le 24 novembre 2008, d'une part, dans les locaux de la société THALES situés 2 rue d'Alembert à Elancourt (78), où était hébergé le dispositif de vote électronique et d'autre part, dans les locaux de la société THALES situés 5-11, rue Blaise Pascal à Elancourt (78), où était située l'équipe de supervision.

[redacted]

En matière de scellement, la délégation de la CNIL a constaté que le scellement physique de la baie de production était partiel : 2 panneaux latéraux pouvaient être ouverts sans rompre le scellé déposé par l'huissier. La baie de secours était physiquement scellée à l'identique. Toutefois, l'accès latéral à celle-ci était rendu difficile du fait qu'elle était positionnée entre deux autres baies. La baie de « supervision et sauvegarde » n'a pas été scellée (ni physiquement ni logiquement).

[redacted]

La délégation de la CNIL a relevé qu'il existait des comptes, dont la création et la gestion étaient sous la responsabilité de la société THALES, pour lesquels aucune procédure logique de scellement n'avait été mise en œuvre. Ces comptes permettaient de se connecter au système de vote pendant le scrutin. Il s'agissait, d'une part, de deux comptes détenus par la société ELECTION EUROPE (selon le ministère, ces comptes étaient en lecture seule). D'autre part, plusieurs comptes, étaient détenus par la société THALES : un compte d'intervention (« Hamdi bis » dont le mot de passe était connu de deux personnes, qui n'étaient pas les administrateurs du système), un compte EC service permettant le basculement du système sur la base de secours et un compte « Mercier » d'accès au serveur de base de données permettant un accès en lecture sur la base de données.

Il a été constaté que ces comptes n'avaient pas fait l'objet de la procédure de scellement (détention d'une partie du mot de passe par huissier de justice). Leur utilisation était uniquement soumise à l'approbation verbale des représentants du ministère et des membres du bureau de vote.

La délégation de la CNIL a relevé, par ailleurs, que le système de prise d'empreintes numériques (ensemble de données identifiant un fichier, en assurant l'intégrité et son absence de modification) ne concernait pas l'intégralité du dispositif de vote.

Enfin, le ministère a considéré que la version actuelle du navigateur Firefox (version 3) n'offrait pas de garanties de confidentialité suffisantes. Selon lui, l'utilisation possible du bouton « page précédente » permettait de connaître les votes précédemment effectués sur le poste. En conséquence, l'utilisation de cette version du navigateur avait été empêchée avant l'ouverture du scrutin. La délégation de la CNIL a toutefois constaté qu'il était possible d'utiliser cette version du navigateur sans corriger l'anomalie soulevée par le ministère :

- sur une plateforme non équipée de Windows (LINUX par exemple) ;
- en modifiant « l'user agent » (identification fournie par le navigateur au moment du chargement des pages web).

D) L'incident du 26 novembre 2008

Dans le journal des votes électroniques, il est indiqué qu'un incident d'une durée de 5 heures avait empêché tout vote le 26 novembre 2008.

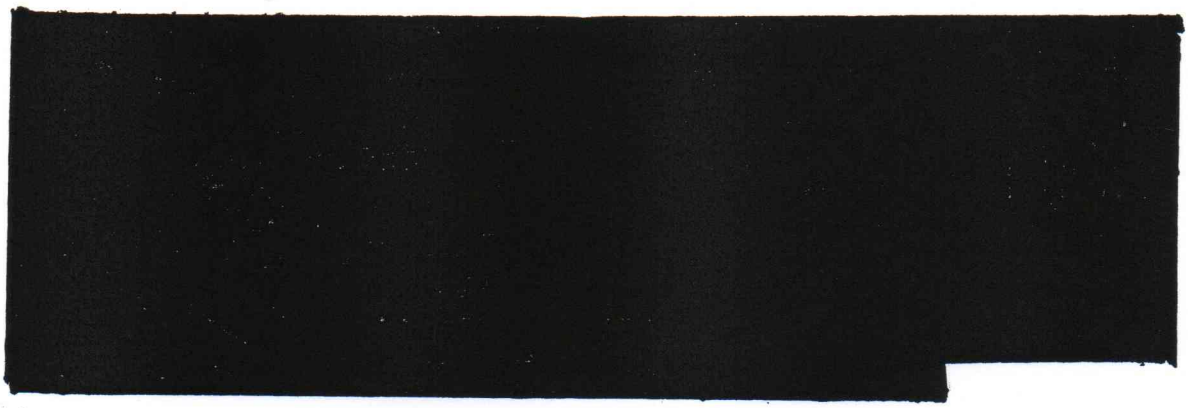
E) Le contrôle du 26 novembre 2008

Une délégation de la CNIL a procédé à un contrôle sur place, le 26 novembre 2008, jour de la clôture du vote électronique, dans les locaux de la société THALES situés 9 rue Baudouin à Paris (75). Un procès-verbal établi par huissier de justice décrit le déroulement des opérations de clôture du vote électronique (voir pièce jointe au courrier du ministère du 2 janvier 2009 annexe 6 précitée).

En matière de modification du dispositif de vote sans descellement, la délégation de la CNIL a constaté que lors de l'ouverture et de la clôture du vote, une intervention par la société THALES, consistant à modifier le système de vote, s'avérait nécessaire afin de permettre l'accès au bouton « voter » par les électeurs au début du vote et de supprimer cet accès à la clôture du vote. Cette action, bien qu'elle visait à modifier le fonctionnement du système de vote, n'a pas nécessité le descellement du système.

En outre, lors de la procédure de clôture du vote électronique, il était prévu une génération du fichier contenant l'ensemble des listes d'émargements à destination des différentes mairies, puis son transfert via une connexion sécurisée au centre d'éditique. Bien que le système ait indiqué un déroulement correct de la procédure, il a été constaté que le fichier n'était pas présent sur le système.

La délégation de la CNIL a constaté un descellement du dispositif de vote par les sociétés ELECTION EUROPE et THALES et une modification du programme de vote sans nouvelle expertise du code source utilisé afin de permettre la génération du fichier. Celui-ci a ensuite été transporté par une personne de la société THALES au centre d'éditique à l'aide d'une clé USB.



F) Le contrôle du 3 décembre 2008

La délégation de la CNIL a procédé à un contrôle sur place, le 3 décembre 2008, jour du dépouillement, dans les locaux de la société THALES situés 9 rue Baudouin à Paris (75). Un procès-verbal établi par huissier de justice décrit le déroulement des opérations de dépouillement (voir pièce jointe au courrier du ministère 2 janvier 2009).

Ce contrôle a permis de faire deux constats principaux. D'une part, s'agissant des opérations de comptage, alors que le président du bureau de vote était connecté au serveur de base de données (urne électronique), afin d'effectuer les opérations de comptage, la délégation a constaté que la société THALES était simultanément connectée sur le serveur de base de données (urne électronique). Les opérations de comptage, dont la durée était estimée initialement à 20 minutes, ont finalement duré environ 3 heures. D'autre part, la délégation de la CNIL a constaté que l'intégrité du scellement de l'urne a été vérifiée après le dépouillement et la proclamation des résultats, et non avant.

Un rapport proposant un avertissement rendu public a été notifié par porteur au ministère du travail, des relations sociales, de la famille et de la solidarité le 25 février 2009, auquel était

jointe la convocation à l'audience du 26 mars 2009. Le rapport de sanction faisait, notamment, état des différents manquements constatés à la loi « informatique et libertés ».

II- Motifs de la décision

Lors de l'audience du 26 mars 2009, le ministère du travail, des relations sociales, de la famille et de la solidarité a présenté à la formation restreinte de la CNIL ses observations, qui s'ajoutaient à celles écrites, parvenues le 24 mars 2009.

A titre liminaire, la Commission rappelle que les systèmes de vote électronique nécessitent la constitution de fichiers comportant des données à caractère personnel au sens de la loi du 6 janvier 1978 modifiée et sont donc soumis à des formalités auprès de la Commission nationale de l'informatique et des libertés (CNIL) préalablement à leur mise en œuvre.

La recommandation de la Commission du 1er juillet 2003, relative à la sécurité des systèmes de vote électronique sur place ou à distance, définit les conditions techniques qui garantissent le respect des principes de protection des données personnelles, en particulier celui du secret du vote. Elle émet un certain nombre de préconisations destinées à assurer l'anonymat et la confidentialité du vote ainsi que la transparence des systèmes informatiques mis en œuvre.

Parmi ses préconisations, la CNIL recommande l'adoption de mesures rigoureuses comme le chiffrement du bulletin de vote dématérialisé dès son émission sur le poste informatique de l'électeur, le recours systématique à l'expertise indépendante des systèmes de vote électronique préalablement à leur mise en œuvre et leur scellement. Il est ainsi possible de s'assurer que le système mis en œuvre est bien celui expertisé. En outre, le système de vote doit être en mesure de fournir la traçabilité complète de son fonctionnement interne lors d'un scrutin afin de garantir une base rigoureuse aux audits externes, notamment en cas de contentieux électoral.

La Commission rappelle que l'article 34 de la loi n° 78-17 du 6 janvier 1978 dispose que le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Au vu des constats précités, résultant de la mise en œuvre de la solution logicielle proposée par la société ELECTION EUROPE, et hébergée par la société THALES, la Commission a constaté les manquements suivants à l'obligation de sécurité et de confidentialité des données.

1) Sur l'expertise et l'identification de la version du logiciel installé

Dans sa recommandation du 1er juillet 2003 sur la sécurité des systèmes de vote électronique, la Commission indique que tout système de vote électronique doit faire l'objet d'une expertise indépendante. Cette expertise permet de vérifier, en particulier, les mesures prises en matière de sécurité et de confidentialité des données.

Dans sa délibération n° 2006-237 du 9 novembre 2006 portant avis sur les projets de décret en Conseil d'Etat et d'arrêté relatifs à l'expérimentation du vote électronique pour les élections prud'homales de 2008, la Commission a souligné que l'obligation d'expertise préalable du système constitue une garantie essentielle de l'intégrité des systèmes de vote électronique.

De surcroit, l'article 10 du décret n° 2007-1130 du 23 juillet 2007 relatif à l'expérimentation du vote électronique pour les élections prud'homales de 2008 à Paris prévoit que le système de vote électronique est soumis, préalablement à sa mise en place, à une expertise indépendante.

L'annexe 5 du rapport d'expertise 10/2008, fournie par le ministère à la Commission, précise que seules certaines parties du code source, indiquées dans ce document comme importantes, ont été expertisées. Lors de la mission de contrôle en date du 19 novembre 2008, la délégation de la CNIL a relevé, par ailleurs, qu'il n'existait pas d'identification de la version du logiciel de vote.

Le rapporteur a constaté que l'absence d'expertise des codes sources dans leur intégralité ne permettait pas de s'assurer du correct fonctionnement du dispositif de vote, fait avéré au travers des différents incidents constatés durant le scrutin. Il a constaté également que l'absence d'identification du logiciel expertisé et du logiciel utilisé durant le scrutin ne garantissait pas que la version expertisée corresponde à celle effectivement utilisée durant le scrutin. En outre, à deux reprises (les 21 et 26 novembre 2008), un dysfonctionnement du système de vote a nécessité sa modification sans qu'il soit procédé à une nouvelle expertise.

Le ministère a indiqué, dans ses observations, que la recommandation précitée de la CNIL ne faisait pas mention de cette exigence. Il a également indiqué que les procès-verbaux des missions de contrôle de la CNIL ne faisaient pas mention de cette absence d'expertise complète.

S'agissant de l'identification des versions expertisées du logiciel de vote, le ministère a considéré que les programmes développés par Election Europe avaient un numéro de version inscrit lorsque les programmes étaient compilés et que ces numéros avaient été contrôlés lors du scellement. Le ministère a indiqué qu'en toute hypothèse, la garantie d'absence de dysfonctionnement d'un ensemble de dispositifs ne pouvait être fondée uniquement sur l'analyse intégrale des codes sources. Il a rappelé qu'en l'espèce, les différents incidents ne sont pas le fait des codes sources du système de vote et qu'ils n'ont jamais affecté le système de vote.

La Commission souligne que la recommandation de la CNIL du 1er juillet 2003 comporte bien cette exigence en son § 3 du point I. 1. Elle indique que les procès-verbaux de contrôle ne font effectivement pas mention du caractère incomplet de l'expertise mais les propres documents fournis par le ministère font apparaître ce caractère non exhaustif, en particulier l'annexe 5 de l'expertise « 10/2008 ».

La Commission constate par ailleurs qu'aucune identification de la version expertisée n'est précisée dans l'expertise. Elle considère, par conséquent, que rien ne permet de garantir que le programme utilisé lors de l'élection est bien celui expertisé.

2) Sur le chiffrement du bulletin de vote

La CNIL a considéré dans sa délibération n° 03-036 du 1er juillet 2003 que *« le bulletin de vote doit être chiffré par un algorithme public réputé « fort » dès son émission sur la machine à voter ou le terminal d'accès à distance et être stocké sur le serveur des votes sans que ce chiffrement n'ait été à aucun moment interrompu »* et que *« la liaison entre le terminal de*

vote de l'électeur et le serveur des votes doit faire l'objet d'un chiffrement pour assurer la sécurité tant du procédé d'authentification de l'électeur que la confidentialité de son vote ».

Ce chiffrement a pour objectif de s'assurer que le bulletin envoyé par l'électeur ne sera pas interrompu, modifié ou lu, à l'image de l'enveloppe dans un vote papier classique.

Par ailleurs, l'article 17 du décret n° 2007-1130 du 23 juillet 2007 relatif à l'expérimentation du vote électronique pour les élections prud'homales de 2008 à Paris dispose notamment que *« le vote est anonyme. Il est chiffré par le système dès son émission sur le terminal utilisé par l'électeur, avant sa transmission au fichier « urne électronique » ».*

Lors de la mission de contrôle en date du 19 novembre 2008, la délégation de la CNIL a constaté que :

- la liaison entre le terminal de vote et le serveur web du système de vote était chiffrée (protocole https),
- une procédure « d'obfuscation » du bulletin de vote entre le navigateur de l'électeur et le serveur d'applications avait été mise en place,
- le bulletin était chiffré par le serveur d'applications en utilisant les clés de dépouillement, lors de son stockage dans l'urne.

Le rapporteur a constaté que le chiffrement de la liaison entre le poste de l'électeur et le serveur web, s'il permet de garantir la confidentialité des informations transmises au système de vote par rapport aux internautes, n'apporte aucune garantie vis-à-vis du prestataire hébergeur du dispositif. De plus, cette liaison chiffrée prenait fin avant que le bulletin ait atteint l'urne puisqu'elle ne couvrait pas la liaison entre le serveur web et le serveur de base de données. Il a également souligné que la méthode « d'obfuscation » ne mettait en œuvre aucun secret. Elle ne pouvait donc être considérée comme un chiffrement fort du bulletin de vote. Il a relevé que même si le bulletin de vote était effectivement stocké chiffré dans l'urne, ce chiffrement n'intervenait qu'au moment de son dépôt dans l'urne.

Le rapporteur a considéré que le dispositif utilisé reposant à la fois sur un brouillage du bulletin (procédure « d'obfuscation ») puis sur un chiffrement de celui-ci, ne correspondait pas aux recommandations de la CNIL dans la mesure où il ne permettait pas de garantir un chiffrement ininterrompu du bulletin de vote entre l'émission de celui-ci depuis le poste de l'électeur et sa réception dans l'urne électronique. Il a indiqué que le dispositif de vote utilisé n'assurait donc pas complètement l'intégrité et la confidentialité du vote.

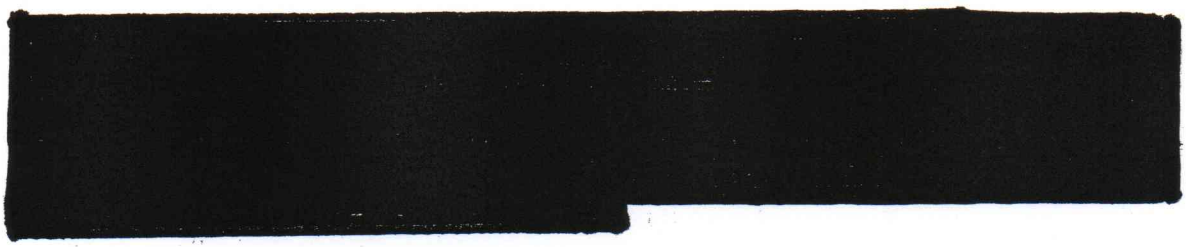
Le ministère a indiqué que la transformation d'obfuscation est paramétrée par une clé et permet la transformation d'un message clair en message codé. [redacted] Le ministère a considéré que le procédé d'obfuscation était donc bien un chiffrement et qu'il comportait un secret. Il a rappelé que le bulletin est bien chiffré durant son parcours jusqu'au système de vote, qu'il restait chiffré dans le serveur web de présentation et qu'il transitait chiffré dans le serveur d'application.

[redacted]

voire un chiffrement. Elle relève également qu'une procédure de chiffrement est mise en oeuvre pour stocker le bulletin de vote dans l'urne électronique. Le chiffrement du bulletin n'est pas, en toute hypothèse, ininterrompu puisqu'une procédure de chiffrement succède à la procédure d'obfuscation. Le temps de cette transformation, même réduit, conduit le bulletin à être en « clair ».

3) Sur le scellement du dispositif de vote

Dans sa recommandation du 1er juillet 2003, la CNIL a considéré que « *Les systèmes de vote électronique expertisés et utilisés doivent faire l'objet d'un scellement c'est à dire d'un procédé permettant de déceler toute modification de ce système. Le procédé de scellement doit lui-même être agréé. La vérification du scellement devrait pouvoir se faire à tout moment, y compris durant le déroulement du scrutin et par tout électeur* ». Ce scellement permet, notamment, de s'assurer que la version expertisée du logiciel est bien celle mise en œuvre. Dans un vote papier classique, ce scellement revient, schématiquement, à vérifier que l'urne est bien vide et de mettre un cadenas dessus avant de commencer le scrutin.



La délégation de la CNIL a constaté lors du contrôle sur place du 24 novembre 2008 un scellement physique partiel du dispositif de vote. En effet, deux panneaux latéraux sur les baies de production et de secours pouvaient être ouverts sans rompre le scellé déposé par l'huissier. De plus, la baie de « supervision et sauvegarde » n'avait pas été scellée tant physiquement que logiquement.

Lors de ce même contrôle, la délégation de la CNIL a constaté que de nombreux comptes de connexion étaient détenus par les sociétés ELECTION EUROPE et THALES. Ces comptes permettaient de se connecter au système de vote pendant le scrutin. Ils n'avaient pas fait l'objet de la procédure de scellement : détention d'une partie du mot de passe par huissier de justice. L'utilisation de ces comptes était uniquement soumise à l'approbation verbale des représentants du ministère et des membres du bureau de vote.

En troisième lieu, de même que les droits associés aux comptes, les droits associés aux groupes auxquels les comptes appartenaient n'ont pas été vérifiés de manière systématique lors du scellement. Or, pour contrôler qu'un utilisateur ne possède pas de droit sur un système, la seule lecture de son nom ou du nom du groupe auquel il appartient n'est pas suffisante mais il faut contrôler effectivement les autorisations que ce compte possède sur les différents éléments constitutifs du système de vote (fichiers, bases de données, accès distant, ...).

En quatrième lieu, lors du contrôle du 24 novembre 2008, la délégation de la CNIL a également constaté que le système de prise d'empreintes numériques ne concernait pas l'intégralité du dispositif de vote. De plus, l'empreinte du système de vote prise lors de la phase de clôture du vote électronique n'a pas pu être comparée à celle prise par l'huissier au début de la période de vote électronique (contrôle du 26 novembre 2008). En effet, les

algorithmes utilisés pour le calcul de l'empreinte au moment du scellement et lors de la phase de clôture du vote électronique n'étaient pas compatibles.

Par conséquent, l'urne électronique ne bénéficiait pas d'un dispositif de verrouillage complet. Les mesures de scellement mises en œuvre ne permettaient, ni de garantir l'absence de modification du dispositif de vote entre le jour du scellement et le jour de la clôture de vote, ni de déceler toute modification du système de vote. La société THALES avait la possibilité, en particulier, d'accéder au dispositif de vote, d'en modifier son fonctionnement, au risque de modifier le résultat des élections, sans qu'il soit nécessaire de le desceller, sans recourir à l'huissier et sans que le bureau de vote ne le sache.

Le rapporteur a considéré que les modifications et les accès au dispositif de vote durant le scrutin soulevaient de graves difficultés en matière de garantie de confidentialité et d'intégrité des votes.

Il a rappelé que la Commission recommande dans sa délibération n° 03-036 du 1er juillet 2003 que la vérification du scellement doit pouvoir se faire à tout moment, y compris durant le déroulement du scrutin, et par tout électeur. Or, il a été constaté, lors du contrôle du 3 décembre 2008, que le scellement de l'urne n'était vérifié qu'après le dépouillement et la proclamation des résultats. Cette vérification aurait dû précéder le dépouillement des votes, de manière à s'assurer que le système n'avait pas été modifié avant de rendre publics les résultats du scrutin.

Le rapporteur a considéré, par conséquent, que ces éléments démontraient que le système de vote électronique adopté ne faisait pas l'objet d'un scellement de nature à garantir la sécurité et la confidentialité des données à caractère personnel des électeurs.

Par ailleurs, lors des missions de contrôle en date des 19 et 26 novembre 2008, la délégation de la CNIL a relevé deux descellements du dispositif de vote, par les sociétés ELECTION EUROPE et THALES, une fois l'urne scellée.

Le rapporteur a considéré que les pratiques qui consistaient à desceller le dispositif de vote et à le modifier durant le scrutin n'étaient pas conformes aux préconisations précitées de la Commission.

Lors du contrôle du 24 novembre 2008, la délégation de la CNIL a constaté que l'utilisation de la version actuelle du navigateur Firefox (version 3) avait été empêchée par le ministère qui considérait qu'elle n'offrait pas de garanties de confidentialité suffisantes.

Toutefois, le rapporteur a constaté que les mesures prises n'étaient pas suffisantes, car son utilisation était possible dans certains cas, et cela, sans qu'il ne soit remédié au risque de rupture de confidentialité.

Le ministère a indiqué, s'agissant de la modification du dispositif de vote du 17 novembre 2008, que seul le serveur Web Présentation, qui fait partie du système de vote, a été descellé et que l'intervention du 21 novembre 2008 n'avait conduit qu'à une correction d'affichage sur le portail d'accès des électeurs. Il rappelle que la CNIL n'avait pas émis d'objection à cette opération.

S'agissant du scellement physique, le ministère a indiqué qu'il avait été corrigé dès le lendemain du passage de la CNIL. Il a ajouté que les bâtiments de Thales étaient soumis à différents niveaux de contrôle d'accès.

S'agissant des comptes permettant d'accéder au système, le ministère a précisé que les comptes de la société Election Europe étaient en lecture seule et que les journaux techniques de l'ensemble du système de vote ont permis aux experts du bureau de vote de contrôler les accès au système de vote durant tout le scrutin. L'utilisation des comptes de la société Thales étaient soumis à l'autorisation du magistrat président du bureau de vote et faisaient l'objet d'une traçabilité et que leurs possibilités d'intervention étaient limitées. De plus, toutes les opérations menées via ces comptes l'ont été après consultation du bureau de vote et des experts de ce bureau. Les vérifications des droits associés aux comptes ont également été effectuées et signalées dans le PV d'huissier Le Honsec.

S'agissant des empreintes numériques, le système de vote a fait l'objet de vérifications d'intégrité durant toute la période de vote. La vérification d'intégrité entre le scellement et la clôture a été faite et régulièrement vérifiée.

Le ministère a ajouté que l'activation et la désactivation du bouton « voter » ne conduisait pas à intervenir sur le système de vote et aucun descellement de ce système n'a été nécessaire à cette fin.

Il a précisé, s'agissant de l'édition des listes d'émargement, que la génération et le transfert de ces listes n'avaient pu être effectués correctement en raison de la désactivation d'un compte interne ce qui a impliqué de relancer cette génération de listes.

S'agissant du comptage et de la connexion de Thales à la base de données, le ministère a indiqué que cette connexion a été utilisée en début de séance pour vérifier l'intégrité de l'urne juste avant son dépouillement et cette connexion est restée ouverte par erreur mais en présence du président du bureau de vote. L'huissier a indiqué qu'aucune autre opération n'avait eu lieu via cette connexion.

Enfin, le ministère a indiqué que l'intégrité du scellement de l'urne a été vérifiée par le président du bureau de vote avant le dépouillement et avant la proclamation des résultats.

[redacted]

S'agissant du descellement du 21 novembre 2008, le compte « Hamdi bis » n'a pas fait l'objet de césure (procédure de scellement) et permet de modifier le formulaire permettant à l'électeur d'exprimer son vote. Elle considère, par conséquent, que le scellement initial n'a pas été correctement effectué et qu'aucun scellement physique et logique du dispositif de secours n'a été mis en place.

La Commission constate que la procédure de contrôle des droits détenus par les utilisateurs s'effectue sur l'appartenance de l'utilisateur à un groupe et que les droits des utilisateurs et des groupes ne sont pas contrôlés.

S'agissant de l'existence de comptes de connexion au dispositif de votes, aucun compte de connexion au système de vote ne devrait exister durant l'élection.

La Commission constate que la sauvegarde sur bande après le dépouillement ne permet pas de garantir que le système n'a pas été modifié durant le vote.

La Commission considère également que les prises d'empreintes numériques ne sont pas valables dans la mesure où le contrôle d'empreinte du bureau de vote s'appuyait uniquement sur le contrôle précédent et non sur l'empreinte initiale et que l'algorithme utilisé lors du scellement et celui du président du bureau de vote ne sont pas compatibles et ne permettent donc pas une comparaison entre le système scellé et le système en cours et en fin de vote.

Le contrôle du scellement par le bureau de vote électronique n'intégrait pas l'intégralité du système de vote, car les procédures stockées (programmes permettant à l'application d'agir sur l'urne) n'y étaient pas intégrées.

Enfin, s'agissant de l'édition des listes d'émargement, la Commission constate que si des garanties ont été prises sur le transfert du fichier au système d'éditique, il n'en demeure pas moins qu'aucune garantie n'est apportée sur l'origine même du fichier.

Sur les manquements constatés

Il résulte de ce qui précède que les garanties apportées par le dispositif de vote mis en place par le ministère du travail, des relations sociales, de la famille et de la solidarité, en terme de sécurité et de confidentialité des données, étaient insuffisantes au regard de l'article 34 de la loi du 6 janvier 1978 modifiée. La Commission considère qu'en n'interdisant pas toute connexion au dispositif de vote durant le scrutin, en ne s'assurant pas que la version expertisée du dispositif de vote était bien celle mise en œuvre, en ne veillant pas au scellement de l'intégralité du dispositif de vote et au chiffrement du bulletin de vote lui-même, le responsable de traitement n'a pas pris toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données. Le manquement à l'article 34 précité est, dès lors, établi.

En conséquence, le ministère du travail, des relations sociales, de la famille et de la solidarité verra prononcer à son encontre un avertissement.

Sur la publicité de la délibération

La Commission considère, en revanche, que les faits de l'espèce ne sont pas de nature à justifier que la délibération à intervenir soit rendue publique.

PAR CES MOTIFS

Conformément aux articles 45 et suivants de la loi du 6 janvier 1978 modifiée, la formation restreinte de la CNIL, après en avoir délibéré, décide de :

- **prononcer à l'encontre du ministre du travail, des relations sociales, de la famille et de la solidarité un avertissement.**