

# Commission nationale de l'informatique et des libertés

## Délibération n° 2009-210 du 30 avril 2009 portant avis sur la mise en place d'un traitement automatisé de données à caractère personnel pour les élections par voie électronique des Français de l'étranger (dossier n° 1349782)

NOR : CNIX0910632X

La Commission nationale de l'informatique et des libertés,

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

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi organique n° 76-97 du 31 janvier 1976 modifiée relative aux listes électorales consulaires et au vote des Français établis hors de France pour l'élection du Président de la République ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004, notamment son article 27-II (4°) ;

Vu la loi n° 82-471 du 7 juin 1982 relative au Conseil supérieur des Français de l'étranger, modifiée par la loi n° 2003-277 du 28 mars 2003 tendant à autoriser le vote par correspondance électronique des Français établis hors de France pour les élections du Conseil supérieur des Français de l'étranger ;

Vu le décret n° 84-252 du 6 avril 1984 modifié portant statut de l'Assemblée des Français de l'étranger et fixant les modalités d'élection de ses membres ;

Vu le décret n° 2003-1377 du 31 décembre 2003 modifié relatif à l'inscription au registre des Français établis hors de France ;

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 en 2007 ;

Vu l'arrêté du 30 mars 2005 relatif au système informatique de traitement des données relatives aux Français établis hors de France ;

Vu la délibération n° 03-036 du 1<sup>er</sup> juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique ;

Vu la délibération n° 2006-042 du 23 février 2006 portant avis sur le traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections à l'Assemblée des Français de l'étranger du 18 juin 2006 ;

Sur le rapport de Mme Isabelle FALQUE-PIERROTIN, vice-présidente, et les observations de Mme Pascale COMPAGNIE, commissaire du Gouvernement,

Emet l'avis suivant :

Le ministère des affaires étrangères souhaite mettre en place un dispositif de vote électronique pour les élections à l'Assemblée des Français de l'étranger (AFE) du 20 mai 2009 relatives aux circonscriptions électorales d'Afrique et d'Amérique.

Pour ce faire, le ministère des affaires étrangères a adressé, le 27 février 2009, à la commission un dossier de formalités préalables comportant un projet de décret et un projet d'arrêté destinés à encadrer réglementairement ce vote électronique ainsi que des éléments techniques relatifs au dispositif de vote électronique retenu.

### *Sur le régime de formalités préalables applicable :*

Aux termes de l'article 27-II (4°) de la loi du 6 janvier 1978 modifiée, sont autorisés par arrêté, ou en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé de la CNIL, « les traitements mis en œuvre par l'Etat ou les personnes morales mentionnées au I aux fins de mettre à disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques ».

Le dispositif de vote électronique proposé par le ministère des affaires étrangères s'effectue par le biais d'un site internet mis à disposition de l'électeur. Ce dispositif constitue donc un téléservice de l'administration électronique.

Les électeurs inscrits sur les listes électorales consulaires sont des usagers de l'administration des affaires étrangères.

Enfin, ce téléservice comporte un identifiant propre à chaque électeur (le numéro d'identifiant consulaire). Il remplit donc toutes les conditions fixées par l'article 27-II (4<sup>o</sup>) de la loi du 6 janvier 1978.

La commission rappelle que, par une délibération n° 03-036 du 1<sup>er</sup> juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, elle a précisé les garanties devant être mises en œuvre pour assurer le secret et l'anonymat du vote. Il convient d'apprécier si, en l'espèce, les caractéristiques du dispositif de vote retenu sont conformes à ces recommandations.

#### *Sur l'expertise indépendante du dispositif de vote électronique :*

La commission relève qu'en application des dispositions de l'article 8 du projet de décret relatif au vote par correspondance électronique des électeurs inscrits sur les listes électorales consulaires en Afrique et en Amérique pour les élections de 2009 à l'Assemblée des Français de l'étranger qui lui est soumis le système de vote doit faire l'objet d'une expertise indépendante. Selon les indications fournies par le ministère, cette expertise sera réalisée avant, pendant et après le scrutin, et ses conclusions seront portées à la connaissance de la CNIL sous forme de rapports détaillés portant notamment sur les garanties apportées à la confidentialité, la sécurité, la sincérité et le contrôle du scrutin.

La commission a reçu le premier rapport d'expertise, réalisé avant le scrutin, en date du 15 avril 2009. Bien que la commission regrette la transmission tardive de ce rapport, elle confirme l'importance que revêt cette expertise dans son travail d'instruction.

#### *Sur la séparation des données identifiantes des électeurs et des votes :*

Le secret du vote doit être garanti par la mise en œuvre de procédés rendant impossible l'établissement d'un lien entre le nom de l'électeur et l'expression de son vote. Il en résulte que la gestion du fichier des votes et celle de la liste d'émargement doivent être faites sur des systèmes informatiques distincts, dédiés et isolés.

L'article 5 du projet de décret prévoit la séparation du fichier des électeurs et de l'urne électronique sur des systèmes informatiques distincts et isolés l'un de l'autre, ce qui est conforme aux recommandations de la CNIL.

#### *Sur le scellement du dispositif de vote :*

Pour permettre aux différents acteurs du scrutin de pouvoir s'assurer à tout moment que le logiciel de vote est bien conforme à celui qui a été préalablement expertisé, la recommandation de la CNIL préconise l'usage d'un « scellement », procédé technique consistant à « signer électroniquement » la version expertisée du logiciel.

L'article 8 du projet d'arrêté prévoit qu'en plus d'un scellement physique des serveurs l'ensemble du système de chaque serveur est scellé en intégrité par calcul d'empreintes numériques.

En outre, le dispositif de chiffrement des bulletins de vote (applet) qui est téléchargé sur l'ordinateur de l'électeur fait l'objet d'une procédure de signature assurant son intégrité par calcul d'empreintes.

Cependant, la commission remarque que, si aucune connexion aux serveurs pendant l'élection n'est possible de la part du prestataire de vote sans l'accord exprès du bureau de vote, l'hébergeur pourra, lui, y accéder dans certaines conditions. En conséquence, la commission estime que ces connexions, qui ne concernent selon le dossier technique que des cas limitativement encadrés, doivent être systématiquement tracées et le traçage, porté immédiatement à la connaissance du bureau de vote et non uniquement mis à disposition de celui-ci.

En tout état de cause, la commission insiste sur le fait que ces connexions ne sauraient conduire à un descellement du système.

#### *Sur la surveillance effective du scrutin :*

La mise en œuvre du système de vote électronique doit être opérée sous le contrôle effectif de représentants du ministère des affaires étrangères responsables du traitement ou d'experts désignés par lui.

En l'espèce, l'article 10 du projet de décret prévoit qu'un bureau central de vote électronique est chargé du contrôle de l'ensemble des opérations de vote électronique et du dépouillement du vote. Il en énumère la composition. Ce bureau, assisté d'un comité technique, veille au bon déroulement technique des opérations électorales et vérifie l'effectivité des dispositifs de sécurité prévus. Ainsi les membres du bureau pourront notamment accéder à tout moment aux locaux hébergeant les traitements.

En outre, toutes les actions concernant le déroulement du vote (interventions sur le système de vote, accès aux locaux hébergeant les traitements) seront enregistrées dans un système de traces dont le bureau de vote pourra, à tout moment, consulter l'historique.

La commission considère ces mesures de contrôle comme satisfaisantes.

#### *Sur la localisation des serveurs du système de vote électronique :*

L'article 7 du projet d'arrêté précise que ce système est localisé sur le territoire métropolitain. La commission souligne l'adéquation de la solution retenue avec sa recommandation de 2003.

*Sur l'authentification des électeurs :*

L'article 6 du projet d'arrêté prévoit que l'authentification des électeurs souhaitant voter par internet sera assurée par le recours à leurs numéros d'identification consulaire et par des mots de passe personnels. Ces mots de passe ne seront pas envoyés pas courrier postal, mais générés par les électeurs après connexion au site internet de l'AFE.

L'obtention du matériel nécessaire au vote par les électeurs se déroule en deux phases :

- depuis le site AFE : après s'être authentifié sur le site portail de l'AFE par son code d'accès et son mot de passe d'adhérent au site, l'électeur crée le mot de passe qui va lui permettre d'accéder à la plate-forme de vote ;
- depuis le portail de vote : l'électeur se connecte sur la plate-forme de vote via son numéro d'identification consulaire et le mot de passe qu'il a créé.

La CNIL considère cette authentification comme satisfaisante.

Cette authentification déclenche la production d'un certificat ainsi que d'un identifiant de vote spécifique à l'électeur (appelé « voter-ID »).

*Sur le chiffrement du bulletin de vote et l'anonymat du vote :*

La commission recommande que le bulletin de vote soit 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. 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 de la confidentialité de son vote.

En l'espèce, il est prévu que, lors du vote, le bulletin soit chiffré sur le poste de l'électeur, dans une enveloppe elle-même signée à l'aide d'un certificat propre à l'électeur et stockée dans l'urne jusqu'au dépouillement.

Préalablement à la phase de dépouillement, la signature est vérifiée puis séparée du bulletin, les bulletins sont ensuite mélangés. Cette phase permet de rompre le lien reliant l'électeur à son bulletin chiffré par le biais de son certificat.

Lors de la phase de dépouillement, les bulletins sont enfin déchiffrés et les votes comptabilisés.

La commission considère que le chiffrement de manière ininterrompue du poste de l'électeur jusqu'à la phase de dépouillement est conforme à ses recommandations.

En revanche, **durant le scrutin, il est théoriquement possible de lier un bulletin chiffré avec un électeur.** En effet, le certificat de l'électeur contient des informations permettant de l'identifier indirectement (via le « voter-ID »). **Cependant, si le risque de levée de l'anonymat existe, il est néanmoins maîtrisé en l'espèce par les garanties apportées par les mesures de sécurité physiques, logiques et organisationnelles mises en place.**

**En tout état de cause, dès la fin du scrutin électronique et avant le dépouillement de celui-ci, le lien entre le bulletin chiffré et le « voter-ID » est rendu impossible par la destruction du serveur d'émargement.**

**Compte tenu des éléments évoqués ci-dessus, la commission insiste sur l'extrême vigilance dont devront faire preuve les organisateurs du scrutin concernant les mesures de sécurité précitées.**

*Sur le dépouillement du vote :*

La CNIL recommande que la génération des clés destinées à permettre le dépouillement des votes soit publique et se déroule le jour du dépouillement. Le nombre de clés doit être au minimum de deux, conservées sous pli scellé jusqu'au dépouillement.

L'article 18 du projet de décret prévoit qu'avant l'ouverture du vote par voie électronique les dix membres titulaires et suppléants du bureau de vote par voie électronique se voient chacun remettre une clé de dépouillement distincte et strictement personnelle.

Chaque clé est stockée sur une carte à puce protégée par mots de passe.

L'article 21 du projet de décret prévoit que, pour permettre le dépouillement, au moins quatre de ces clés doivent être réunies.

La commission estime en conséquence que ce dispositif de dépouillement est d'un niveau de sécurité satisfaisant à la condition que ces mesures puissent être vérifiées par l'expertise indépendante.

*Sur le contrôle du vote a posteriori :*

Une opération de sauvegarde de l'urne est réalisée en fin de scrutin et avant le dépouillement de l'urne, pour faire face à d'éventuels recours.

Ainsi, pour permettre de procéder à nouveau au décompte des votes sans faire appel aux membres du bureau de vote, le ministère s'engage à conserver les cartes à puce, sur lesquelles sont stockées les clés de dépouillement, et ce dans les mêmes conditions de sécurité que celles utilisées pour la conservation de l'urne.

La commission prend acte enfin que l'article 22 du projet de décret prévoit qu'à l'expiration du délai de recours ou après l'intervention d'une décision juridictionnelle devenue définitive il sera procédé à la destruction des sauvegardes sous le contrôle du bureau de vote.

*Le président,*  
A. TÜRK