Commission Nationale de l'Informatique et des Libertés (CNIL)

Délibération n° 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

01 Juillet 2003 - Thème(s) : Citoyenneté

La Commission nationale de l'informatique et des libertés,

Vu la convention 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 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 des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pris ensemble le décret d'application n° 78-774 du 17 juillet 1978 ;

Vu le code électoral ;

Après avoir entendu Monsieur Maurice BENASSAYAG, commissaire, en son rapport et Madame Charlotte-Marie PITRAT, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La Commission constate le développement de systèmes de vote électronique sur place ou à distance tendant à faciliter l'expression du vote et les opérations matérielles de dépouillement.

Le recours à de tels systèmes qui nécessitent la mise en œuvre de traitements automatisés d'informations nominatives, au sens de l'article 5 de la loi du 6 janvier 1978, pour le fichier informatique des électeurs, le traitement automatisé des résultats (pour les données nominatives relatives aux candidats) ou la constitution de la liste d'émargement doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin sauf pour les scrutins publics, le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l'élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

La présente recommandation porte sur les conditions techniques propres à garantir les principes fondamentaux préalablement énumérés et à assurer la sécurité des systèmes de vote électronique. Il appartient au législateur de définir les conditions juridiques de la mise en œuvre du vote électronique.

Elle a pour champ d'application les dispositifs de vote électronique sur place et à distance, en particulier par internet. Elle ne concerne pas les dispositifs de vote par codes-barres et les dispositifs de vote par téléphone fixe ou mobile sur lesquels la Commission sera amenée à se prononcer.

La recommandation prend appui essentiellement sur les dossiers qui ont été soumis à la Commission dans le cadre des formalités préalables prévues par la loi du 6 janvier 1978. Elle constitue une première approche de systèmes qui sont encore en pleine évolution. Elle est destinée à orienter cette évolution dans le sens du respect des principes de protection des données personnelles et à éclairer les responsables des scrutins pour le choix des dispositifs de vote électronique.

Compte tenu de ces observations préalables, la Commission émet la recommandation suivante :

I/ Sur les exigences préalables à la mise en œuvre des systèmes de vote électronique

1. L'expertise du système de vote électronique

Tout système de vote électronique devrait faire l'objet :

- d'une procédure d'agrément par le ministère de l'intérieur pour les machines à voter définies par le code électoral ;

- d'une expertise indépendante pour les autres systèmes.

Le rapport d'expertise devra être joint aux formalités préalables à accomplir auprès de la CNIL.

La Commission estime que dans le cas d'une élection organisée par une collectivité publique, le code source des logiciels utilisés par le système de vote électronique devrait être accessible sans restriction, afin de permettre la réalisation de toutes les expertises jugées nécessaires.

Dans l'hypothèse de l'utilisation d'un logiciel libre, quelle que soit la personne mettant en œuvre le traitement, ce logiciel doit être expertisé.

Afin de garantir un contrôle effectif des opérations électorales, le prestataire technique doit mettre à disposition des représentants de l'organisme responsable du traitement, des experts, des membres du bureau de vote, des délégués des candidats et des scrutateurs tous documents utiles et assurer une formation de ces personnes au fonctionnement du dispositif de vote électronique.

2. La séparation des données nominatives 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. Ces fichiers doivent faire l'objet de mesures de chiffrement selon un algorithme public réputé « fort ».

3. Les sécurités informatiques

Il convient que toutes les mesures physiques (contrôle d'accès, détermination précise des personnes habilitées à intervenir…) et logiques (firewall, protection d'accès aux applicatifs…) soient prises tant au niveau des serveurs du dispositif que sur les postes accessibles au public afin de garantir la sécurité et la confidentialité des données personnelles en particulier contre les intrusions venant de l'extérieur. Les algorithmes de chiffrement, de signature électronique et les fonctions de hachage doivent être des algorithmes publics réputés « forts ».

4. Le scellement du dispositif de vote électronique

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.

5. L'existence d'une solution de secours

Tout système de vote électronique devrait comporter un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques.

6. La surveillance effective du scrutin

La mise en œuvre du système de vote électronique doit être opérée sous le contrôle effectif, tant au niveau des moyens informatiques centraux que de ceux, éventuellement, déployés sur place, de représentants de l'organisme mettant en place le vote ou d'experts désignés par lui. Dès lors, il importe que toutes les mesures soient prises pour leur permettre de vérifier l'effectivité des dispositifs de sécurité prévus pour assurer le secret du vote et, en particulier, les mesures prises respectivement pour :

- garantir la confidentialité du fichier des électeurs comportant les éléments d'authentification,
- procéder au chiffrement des bulletins de vote et à leur conservation dans un traitement distinct de celui mis en oeuvre pour assurer la tenue du fichier des électeurs,
- assurer la conservation des différents supports d'information pendant et après le déroulement du scrutin.

Toutes les facilités devraient être accordées aux membres du bureau de vote et aux délégués des candidats, s'ils le souhaitent, pour pouvoir assurer une surveillance effective de l'ensemble des opérations électorales et, en particulier, de la préparation du scrutin, du vote, de l'émargement et du dépouillement.

7. La localisation du système informatique central

Il paraît hautement souhaitable que les serveurs et les autres moyens informatiques centraux du système de vote électronique soient localisés sur le territoire national afin de permettre un contrôle effectif de ces opérations par les membres du bureau de vote et les délégués ainsi que l'intervention, le cas échéant, des autorités nationales compétentes.

II/ Sur le scrutin

A/ Sur les opérations précédant l'ouverture du scrutin

1. La confidentialité des données

Les fichiers nominatifs des électeurs constitués aux fins d'établir la liste électorale, d'adresser le matériel de vote et de réaliser les émargements ne peuvent être utilisés qu'aux fins précitées et ne peuvent être divulgués sous peine des sanctions pénales encourues au titre des articles 226-17 et 226-21 du code pénal.

La confidentialité des données est également opposable aux techniciens en charge de la gestion ou de la maintenance du système informatique.

Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement/déchiffrement et le contenu de l'urne ne doivent pas être accessibles, de même que la liste d'émargement, sauf aux fins de contrôle de l'effectivité de l'émargement des électeurs.

En cas de recours à un prestataire extérieur, celui-ci doit s'engager contractuellement à respecter ces dispositions par la signature d'une clause de confidentialité et de sécurité et à fournir le descriptif détaillé du dispositif technique mis en œuvre pour assurer cette confidentialité. Le prestataire doit également s'engager à restituer les fichiers restant en sa possession à l'issue des opérations électorales et à détruire toutes les copies totales ou partielles qu'il aurait été amené à effectuer sur quelque support que ce soit.

Le recours à une télé-maintenance des matériels et logiciels ne devrait pas être possible durant tout le scrutin et jusqu'à l'épuisement des délais légaux de recours contentieux.

2. Les procédés d'authentification de l'électeur

La Commission estime que dans le cas d'élections où un vote à distance a été prévu par le législateur, une authentification de l'électeur sur la base d'un certificat électronique constitue la solution la plus satisfaisante en l'état de la technique. Le tiers certificateur doit être un organisme indépendant professionnellement reconnu.

Dans l'état actuel des textes, le recours à l'enregistrement de données biométriques à des fins de constitution d'un fichier électoral pour s'assurer de l'identité de l'électeur et de l'unicité de son vote ne peut s'envisager que si la donnée biométrique figure dans la catégorie de celles ne laissant pas de traces ou que si cet enregistrement s'effectue sur un support individuel détenu par l'électeur et ne donne pas lieu à la constitution d'un fichier de données biométriques.

A défaut de recourir aux solutions précitées, dans le cas de la génération d'identifiants et de mots de passe à partir de la liste électorale, le fichier ainsi créé doit faire l'objet d'un chiffrement. Les modalités de génération et d'envoi des codes personnels doivent être conçues de façon à garantir leur confidentialité et en particulier que les divers prestataires éventuels ne puissent en prendre connaissance.

Dans le cas où le vote s'opérerait par l'enregistrement d'un identifiant permanent apposé sur une carte ou tout autre document ainsi qu'un mot de passe envoyé à chaque vote, la génération de ces identifiants et mots de passe devrait se faire dans les mêmes conditions de sécurité que celles énumérées ci-dessus. Il en va de même de l'envoi du mot de passe.

L'authentification de l'électeur peut être renforcée par un dispositif de type défi/réponse, c'est à dire l'envoi par le serveur d'authentification d'une question dont l'électeur devrait connaître la réponse.

3. L'information des électeurs

Il convient de fournir aux électeurs en temps utile une note explicative détaillant clairement les opérations de vote ainsi que le fonctionnement général du système de vote électronique.

4. Le test du système avant l'ouverture du scrutin

Un test du système de vote électronique doit être organisé avant l'ouverture du scrutin et en présence des scrutateurs afin de constater la présence du scellement, le bon fonctionnement des machines, la remise à zéro du compteur des voix et que l'urne électronique destinée à recevoir les votes est bien vide et scellée.

5. Les clés de dépouillement de vote

La génération des clés destinées à permettre le dépouillement des votes à l'issue du scrutin doit être publique et se dérouler le jour du dépouillement. Cette procédure devrait être conçue de manière à prouver de façon irréfutable que seuls le président du bureau et ses assesseurs prennent connaissance de ces clés, à l'exclusion de toute autre personne y compris les personnels techniques chargés du déploiement du système de vote. La Commission estime que le nombre de clés de chiffrement doit être au minimum de trois, la présence de deux titulaires de ces clés étant indispensable pour autoriser le dépouillement. Elle considère que les clés doivent ensuite être conservées sous pli scellé sous la responsabilité du président du bureau de vote qui les remet, lors de la clôture du scrutin, aux membres du bureau désignés, contre accusé de réception.

Le système de vote doit garantir que des résultats partiels (hormis le nombre de votants) ne seront pas accessibles durant le déroulement du vote.

B/ Sur le déroulement du vote

1. Le vote

Les heures d'ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Pour se connecter à distance ou sur place au système de vote, l'électeur doit se faire reconnaître par un dispositif d'authentification établi conformément à la présente recommandation, permettant au serveur de vérifier son identité et s'il n'a pas déjà voté.

L'électeur accède aux listes ou aux candidats officiellement retenus et dans l'ordre officiel. Le vote blanc doit être prévu lorsque la loi l'autorise.

L'électeur doit pouvoir choisir une liste, un candidat ou un vote blanc de façon à ce que ce choix apparaisse clairement à l'écran indépendamment de toute autre information. Il devrait avoir la possibilité de revenir sur ce choix.

Il valide ensuite son choix et cette opération déclenche l'envoi du bulletin de vote dématérialisé vers le serveur des votes.

L'électeur devrait recevoir immédiatement confirmation de son vote et avoir la possibilité de conserver une trace de cette confirmation.

2. Le chiffrement du bulletin de vote

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. 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.

3. L'émargement

L'émargement doit se faire dès la validation du vote de façon à ce qu'un autre vote ne puisse intervenir à partir des éléments d'authentification de l'électeur déjà utilisés. L'émargement comporte un horodatage. La liste d'émargement doit être située sur un système distinct de celui contenant l'urne électronique. Cette liste, aux fins de contrôle de l'émargement, ainsi que le compteur des votes ne doivent être accessibles qu'aux membres du bureau de vote et aux personnes autorisées.

La liste d'émargement doit être enregistrée sur un support scellé, non réinscriptible, rendant ainsi son contenu inaltérable et probant.

4. Le dépouillement

Le dépouillement est actionné par les clés de déchiffrement, remises par le président du bureau de vote après la clôture des opérations de vote aux membres du bureau dûment désignés au moment de la génération de ces codes. Les membres du bureau doivent actionner publiquement le processus de dépouillement.

Les décomptes des voix par candidat ou liste de l'élection doivent apparaître lisiblement à l'écran et faire l'objet d'une édition sécurisée pour être portés au procès-verbal de l'élection. Le cas échéant, l'envoi des résultats à un bureau centralisateur à distance devrait s'effectuer selon une liaison sécurisée empêchant toute captation ou modification des résultats.

Le système de vote électronique doit être bloqué après le dépouillement de sorte qu'il soit impossible de reprendre ou de modifier les résultats après la décision de clôture du dépouillement prise par la commission électorale.

III/ Sur le contrôle des opérations de vote a posteriori par le juge électoral

1. Les garanties minimales pour un contrôle a posteriori

Pour les besoins d'audit externe, notamment en cas de contentieux électoral, le système de vote électronique doit être capable de fournir les éléments techniques permettant au minimum de prouver de façon irréfutable que :

- durant le scrutin le procédé de scellement est resté fiable ;
- les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls titulaires ;
- le vote est anonyme ;
- la liste d'émargement ne comprend que les électeurs ayant voté ;
- l'urne dépouillée est bien celle contenant les votes des électeurs et elle ne contient que ces votes ;
- aucun décompte partiel n'a pu être effectué durant le scrutin ;
- la procédure de décompte des votes enregistrés doit pouvoir être déroulée de nouveau.

2. La conservation des données portant sur l'opération électorale

Tous les fichiers supports (copies des programmes sources et exécutables, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) doivent être conservés sous scellés jusqu'à l'épuisement des délais de recours contentieux. Cette conservation doit être assurée sous le contrôle de la commission électorale dans des conditions garantissant le secret du vote. Obligation doit être faite, le cas échéant, au prestataire de service de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation des supports. Lorsque aucune action contentieuse n'a été engagée avant l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.

Dans la phase d'expérimentation des systèmes de vote électronique, la CNIL demandera qu'un bilan de la mise en œuvre du dispositif de vote électronique utilisé soit établi à brève échéance suivant le déroulement de l'élection et lui soit adressé.

Le Président

Michel GENTOT