Commission nationale de l'informatique et des libertés

Délibération nº 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

NOR : *CNIA1000012X*

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 le code électoral ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi nº 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu le décret nº 2005-1309 du 20 octobre 2005 pris pour l'application de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret nº 2007-451 du 25 mars 2007 ;

Après avoir entendu Mme Isabelle Falque-Pierrotin, vice-présidente, en son rapport et Mme Elisabeth Rolin, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Alors que le vote électronique commençait seulement à s'implanter en 2003, lors de l'adoption de la première recommandation de la CNIL, la commission constate aujourd'hui que les systèmes de vote électronique sur place ou à distance se sont développés et s'étendent désormais à un nombre croissant d'opérations de vote et de types de vote.

La commission souligne que le recours à de tels systèmes 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 commission constate que si l'application principale du vote électronique réside dans les élections professionnelles (comité d'entreprise et représentants du personnel), celui-ci se développe également pour les assemblées générales, conseil de surveillance, élection des représentants de professions réglementées et, depuis 2003, pour des élections à caractère politique. De plus, en 2009, pour la première fois, la possibilité de recourir au vote électronique pour une élection nationale, au suffrage universel direct, a été introduite par l'ordonnance nº 2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France.

Devant l'extension du vote par internet à tous types d'élections, la commission souhaite rappeler que le vote électronique présente des difficultés accrues au regard des principes susmentionnés pour les personnes chargées d'organiser le scrutin et celles chargées d'en vérifier le déroulement, principalement à cause de la technicité importante des solutions mises en œuvre. Au cours des travaux que la commission a menés depuis 2003, elle a, en effet, pu constater que les systèmes de vote existants ne fournissaient pas encore toutes les garanties exigées par les textes légaux. Dès lors et en particulier, compte tenu des éléments précités, la commission est réservée quant à l'utilisation de dispositifs de vote électronique pour des élections politiques.

La présente délibération a pour objet de revoir la recommandation de 2003 à l'aune des opérations électorales intervenues depuis cette date et de leur analyse par la CNIL, y compris par les contrôles effectués.

La nouvelle recommandation a pour champ d'application les dispositifs de vote électronique à distance, en particulier par internet. Elle ne concerne pas les dispositifs de vote par codes-barres, les dispositifs de vote par téléphone fixe ou mobile, ni les machines à voter. Elle est destinée à fixer, de façon pragmatique, les garanties minimales que doit respecter tout dispositif de vote électronique, celles-ci pouvant être, le cas échéant, complétées par des mesures supplémentaires. Elle vise également à orienter les futures évolutions des systèmes de vote électronique en vue d'un meilleur respect des principes de protection des données personnelles et à éclairer les responsables de traitement sur le choix des dispositifs de vote électronique à retenir.

Elle abroge la délibération nº 2003-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes 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 doit faire l'objet d'une expertise indépendante.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des mesures décrites dans la présente délibération, et notamment sur :

– le code source du logiciel, y compris dans le cas de l'utilisation d'un logiciel libre ;
– les mécanismes de scellement utilisés aux différentes étapes du scrutin (voir ci-après) ;
– le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
– les échanges réseau ;
– les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur.

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 ;
– avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d'expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondant à la première version et aux évolutions substantielles de la solution de vote mise en place.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

L'expert doit fournir un moyen technique permettant de vérifier *a posteriori* que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise.

2. *La séparation des données nominatives des électeurs et des votes*

Le dispositif doit garantir que l'identité de l'électeur ne peut pas être mise en relation avec l'expression de son vote, et cela à tout moment du processus de vote, y compris après le dépouillement.

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 des données personnelles et du système de vote dans son ensemble. Les algorithmes de chiffrement et de signature électronique doivent, dans tous les cas, être des algorithmes publics réputés « forts » et doivent, si les élections sont mises en place par une autorité administrative, répondre aux exigences prévues dans le référentiel général de sécurité (RGS).

Si un système matériel permet d'héberger plusieurs scrutins, il doit mettre en œuvre une solution technique (par exemple par une « virtualisation » des systèmes) permettant d'isoler chaque scrutin sur un système informatique distinct de manière à garantir que chaque système soit indépendant et se comporte de manière autonome.

4. *Le scellement du dispositif de vote électronique*

Avant le début du scrutin, les systèmes de vote électronique utilisés, la liste des candidats et la liste des électeurs doivent faire l'objet d'un scellement, c'est-à-dire d'un procédé permettant de déceler toute modification du système. Avant cette procédure de scellement, il est vérifié que les modules ayant fait l'objet d'une expertise n'ont pas été modifiés. La liste d'émargement et l'urne électronique doivent faire l'objet d'un procédé garantissant leur intégrité durant le vote, c'est-à-dire assurant qu'ils ne peuvent respectivement être modifiés que par l'ajout d'un bulletin et d'un émargement, dont l'intégrité est assurée, d'un électeur authentifié de manière non frauduleuse. Ce procédé doit déceler toute autre modification du système. Après la clôture du vote, la liste d'émargement et l'urne électronique doivent être scellées.

Les procédés de scellement doivent eux-mêmes utiliser des algorithmes publics réputés forts et, le cas échéant, respecter les recommandations du référentiel général de sécurité. La vérification des scellements doit

pouvoir se faire à tout moment, y compris durant le déroulement du scrutin. Le bureau de vote doit disposer d'outils dont l'utilisation ne requiert pas l'intervention du prestataire pour procéder à la vérification du scellement, par exemple par une prise d'empreinte numérique.

5. *L'existence d'une solution de secours*

Tout système de vote électronique doit 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 pour :

– garantir la confidentialité du fichier des électeurs comportant les éléments d'authentification ;
– garantir le chiffrement ininterrompu des bulletins de vote et leur conservation dans un traitement distinct de celui mis en œuvre 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 doivent 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.

A ce titre et 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.

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 prestataire peut recevoir automatiquement des informations techniques sur le fonctionnement du système de vote pendant tout le déroulement du scrutin. Le prestataire ne doit intervenir sur le système de vote qu'en cas de dysfonctionnement informatique résultant d'une attaque du système par un tiers, d'une infection virale, d'une défaillance technique ou d'une altération des données. Un dispositif technique doit garantir que le bureau de vote est informé automatiquement et immédiatement de tout accès par le prestataire à la plate-forme de vote. Le prestataire doit informer le bureau de vote de toutes les mesures prises pour remédier au dysfonctionnement constaté. Le système de vote doit comprendre un module permettant la remontée automatique de cette information au bureau de vote.

Toutes les actions effectuées sur le serveur de vote ainsi que celles concernant le déroulement du scrutin doivent faire l'objet d'une journalisation. L'intégrité de cette journalisation doit être garantie à tout moment par un procédé cryptographique.

Le bureau de vote, quant à lui, a compétence pour prendre toute mesure d'information et de sauvegarde, et notamment pour décider la suspension des opérations de vote. Le système de vote doit permettre d'informer les électeurs de cette éventuelle décision.

2. *Les procédés d'authentification de l'électeur*

Le système de vote doit prévoir l'authentification des personnes autorisées à accéder au système pour exprimer leur vote. Il doit garantir la confidentialité des moyens fournis à l'électeur pour cet accès et prendre toutes précautions utiles afin d'éviter qu'une personne non autorisée ne puisse se substituer frauduleusement à l'électeur.

La commission estime qu'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 certificat électronique doit être choisi et utilisé conformément aux préconisations du RGS.

Dans le cas du recours à un dispositif biométrique pour l'authentification, le responsable de traitement doit respecter les formalités imposées par la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

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 pas 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 électeur, la génération de ces identifiants et mots de passe doit 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 est seul à connaître la réponse – ou par l'envoi d'un code par SMS sur le téléphone personnel de l'électeur.

En cas de perte ou de vol de ses moyens d'authentification, une procédure doit permettre à l'électeur d'effectuer son vote et de rendre les moyens d'authentification perdus ou volés inutilisables.

Le vote doit être accessible à tous les systèmes d'exploitation et tous les navigateurs utilisés par les électeurs. A défaut de mettre à disposition du matériel de vote accessible à tous, une procédure manuelle doit être prévue.

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 contrôle du système avant l'ouverture du scrutin*

Un contrôle du système de vote électronique doit être organisé avant l'ouverture du scrutin et en présence des scrutateurs afin de constater la présence des différents scellements, le bon fonctionnement des machines, que la liste d'émargement est vierge et que l'urne électronique destinée à recevoir les votes est bien vide.

5. *Les clés de chiffrement*

La génération des clés destinées à permettre le déchiffrement des bulletins de vote doit être publique et se dérouler avant l'ouverture du scrutin. Cette procédure doit 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 combinaison d'au moins deux de ces clés étant indispensable pour permettre le dépouillement.

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

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 s'authentifier conformément à la présente recommandation. Au cours de cette procédure, le serveur de vote vérifie l'identité de l'électeur et que celui-ci est bien autorisé à voter. Dans ce cas, il 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 doit 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 doit 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 le poste de l'électeur et être stocké dans l'urne, en vue du dépouillement, sans avoir été déchiffré à aucun moment, même de manière transitoire. La liaison entre le terminal de vote de l'électeur et le serveur des votes doit faire l'objet d'un chiffrement distinct de celui qui s'applique au bulletin pour assurer la sécurité tant du procédé d'authentification de l'électeur que la confidentialité de son vote. La mise en place du canal de communication doit intégrer une authentification du serveur de vote.

Par ailleurs, le stockage du bulletin dans l'urne ne doit pas comporter d'horodatage, pour éviter tout rapprochement avec la liste d'émargement.

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. 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.

4. *Le dépouillement*

La fermeture du scrutin doit immédiatement être suivie d'une phase de scellement de l'urne et de la liste d'émargement, phase qui précède le dépouillement. L'ensemble des informations nécessaires à un éventuel contrôle *a posteriori* doit également être recueilli lors de cette phase. Ces éléments sont enregistrés sur un support scellé, non réinscriptible et probant.

Le dépouillement est actionné par les clés de déchiffrement, remises aux membres du bureau dûment désignés au moment de la génération de ces clés. 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, c'est-à-dire d'un mécanisme garantissant que l'affichage et l'impression des résultats correspondent au décompte de l'urne, pour être portés au procès-verbal de l'élection. Le cas échéant, l'envoi des résultats à un bureau centralisateur à distance doit s'effectuer par 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 :

– le procédé de scellement est resté intègre durant le scrutin ;
– les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls titulaires ;
– le vote est anonyme ;
– la liste d'émargement ne comprend que la liste des 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. Lorsqu'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.

IV. – **La publication**

La présente délibération sera publiée au *Journal officiel* de la République française.

Le président,
A. TÜRK