ANNEXE I

Délibération de la Commission nationale de l'informatique et des libertés n° 98-041 du 28 avril 1998 portant recommandation sur l'utilisation des systèmes de vote par codes-barres dans le cadre d'élections par correspondance pour les élections professionnelles

« La Commission nationale de l'informatique et des libertés,
Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu le code électoral ;
Vu le code de la sécurité sociale, et notamment les articles L. 911-1 et suivants et R. 641-13 à R. 641-28 ; Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 29 ;
Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 susvisée ;
Après avoir entendu M. Bouchet (Hubert) en son rapport et Mme Pitrat (Charlotte-Marie) en ses observations ;
Considérant que divers organismes recourent, dans le souci de faciliter l'expression du vote et les opérations matérielles de dépouillement, à des systèmes de dépouillement automatique des bulletins ; que tel est le cas pour certaines élections professionnelles par correspondance, lorsque le nombre d'électeurs est élevé ;
Considérant que ces systèmes reposent sur le décompte automatique de bulletins qui comportent des données codées - généralement des codes-barres - permettant l'identification de l'électeur et des données codées exprimant son choix ; que le recours à de tels systèmes nécessite la mise en œuvre de traitements automatisés d'informations nominatives, au sens de l'article 5 de la loi du 6 janvier 1978, qu'il s'agisse du fichier informatique des électeurs, du traitement automatisé des résultats ou de la constitution de la liste d'émargement ;
Considérant que le recours aux systèmes de vote par codes-barres et de dépouillement automatique des votes ne peut être admis que si le secret du vote, la sincérité des opérations électorales, la surveillance effective du scrutin et le contrôle a posteriori par le juge de l'élection garantissent le principe de la liberté du scrutin,

« Recommande :

I. - Organisation des élections

Le recours à un système de dépouillement automatique des votes par lecture de codes-barres doit être expressément mentionné dans le protocole d'accord préélectoral conclu entre les organisations syndicales sous le contrôle de la direction de l'organisme.
Lorsque l'organisme relève des articles L. 911-1 ou R. 641-13 et suivants du code de la sécurité sociale, le protocole établi par la direction de l'organisme doit mentionner le recours à un système de dépouillement automatique des votes.
Ce protocole doit notamment préciser les conditions techniques de mise en œuvre du système, les dispositions prises pour garantir le secret du vote et la sincérité des opérations électorales, les modalités pratiques d'acheminement des documents de vote (routage) et les critères généraux de détermination des votes blancs ou nuls.
A cet effet, il importe que toutes dispositions soient prises afin de permettre aux représentants du corps électoral d'assurer une surveillance effective de l'ensemble des opérations électorales et, en particulier, de la préparation du scrutin, du dépouillement et de l'émargement.
En cas de recours à un prestataire extérieur, une copie du cahier des charges doit être jointe au protocole.

Un expert informatique figurant sur la liste établie par la Cour de cassation ou sur les listes établies par les cours d'appel peut être chargé par la direction de l'organisme de vérifier préalablement à l'élection que le système informatique qui sera utilisé respecte les dispositions énumérées ci-après et s'en assurer le jour du dépouillement. Dans le cas où il est recouru à un tel expert, mention doit en être faite dans le protocole. En outre, la commission électorale, le cas échéant assistée d'un huissier de justice, devra être présente, assistée de l'éventuel expert informatique, lors des opérations de dépouillement et d'émargement, afin de dresser un rapport sur le déroulement du scrutin, auquel seront joints le rapport de vérification préalable et, le cas échéant, les observations de l'expert susmentionné.

II. - Préparation du scrutin

1/ Les fichiers nominatifs d'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. En cas de recours à un prestataire extérieur, celui-ci doit s'engager contractuellement à respecter ces dispositions, à restituer les fichiers dès la fin des opérations et s'engager à détruire toutes les copies totales ou partielles qu'il aurait été amené à effectuer sur quelque support que ce soit.

2/ 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 :

- l'électeur ne doit être identifié sur la carte exprimant son vote que par un numéro spécifique généré de façon aléatoire, à l'exclusion de toute autre information. Ce numéro doit être modifié pour chaque scrutin ;
- le fichier de correspondance, établi pour permettre l'édition de la liste d'émargement, entre le nom des électeurs et les numéros qui leur sont attribués doit être conservé sous le contrôle de la commission électorale ;
- les documents de vote transmis par l'électeur doivent être conçus de façon que le numéro qui permet son identification et le sens du vote exprimé fassent l'objet de lectures distinctes de sorte qu'il soit impossible techniquement d'établir un lien entre ces deux informations ;
- les documents de vote transmis par l'électeur doivent l'être sous pli clos.

3/ Toutes précautions utiles doivent être prises afin que les cartes de vote par correspondance ne subissent, lors de leur envoi par les électeurs, aucune altération de nature à empêcher la comptabilisation du vote ou à considérer le vote comme étant nul. Il en résulte que :

- l'envoi du matériel de vote aux électeurs doit être accompagné d'une note explicative détaillant de façon claire les modalités des opérations de vote et, en particulier, les critères de comptabilisation et de détermination des votes nuls ou blancs ;
- au cas où l'expression de vote serait matérialisée par l'apposition sur la carte de vote d'une étiquette comportant un code-barres identifiant le candidat, cette étiquette ne doit pouvoir être décollée sans être irrémédiablement altérée.

III. - Dépouillement

1/ A l'issue des opérations de vote mais avant le dépouillement, un test doit être réalisé sur un lot aléatoire de bulletins, sous la conduite de la commission électorale.

2/ Les opérations de dépouillement doivent être effectuées par un ordinateur isolé ou plusieurs ordinateurs reliés en réseau local, ces ordinateurs ne devant en aucun cas comporter le fichier nominatif des votants ni le ou les fichiers de correspondance entre le nom des électeurs et les numéros qui leur sont attribués aléatoirement.

3/ Une solution de secours comportant notamment un dispositif complémentaire en cas de défaillance du système doit être prévue.

4/ Le système doit comporter un dispositif technique rejetant tout bulletin déjà lu.

5/ Le système automatisé 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.

6/ Les voix doivent être comptabilisées par lot de sorte que les expressions individuelles de vote ne puissent être isolées et rapprochées de l'identité du votant.

IV. - Emargement

Le rapprochement du fichier des numéros attribués aux électeurs et du fichier nominatif des électeurs, nécessaire pour l'établissement de la liste d'émargement, doit être réalisé en présence de la commission électorale assistée de l'éventuel expert informatique. La liste d'émargement ne comporte que l'identité des électeurs telle que prévue aux articles L. 18 et L. 19 du code électoral ou par le protocole, le cas échéant, l'identification du collège électoral, ainsi que la mention attestant la participation au vote, à l'exclusion de toute autre information.

V. - Contrôle a posteriori par le juge de l'élection

Tous les fichiers supports (copie des programmes source 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 services de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation des supports. Sauf action contentieuse née avant l'épuisement des délais de recours, il est procédé à la destruction de ces documents sous le contrôle de la commission électorale. »

ANNEXE II

Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet

NOR : CNIL1917529X
JORF n°0142 du 21 juin 2019
Texte n° 95

Version initiale

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 le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;
Vu le code électoral ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article
11-I-2°-a bis) ;
Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Article

Après avoir entendu Mme Dominique CASTERA, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;
Formule les observations suivantes :
À titre liminaire, la commission observe que le constat, réalisé lors de l'adoption de sa recommandation de 2010, du développement et de l'extension des systèmes de vote par correspondance électronique, notamment via Internet, à un nombre croissant d'opérations de vote et de types de vote, reste d'actualité.
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 et libre 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 par correspondance électronique, notamment via Internet, doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.
Devant l'extension continue du vote par Internet à tous types d'élections, la commission souhaite rappeler que le vote par correspondance électronique, notamment via Internet, 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 l'opacité et de la technicité importante des solutions mises en œuvre, ainsi que de la très grande difficulté de s'assurer de l'identité et de la liberté de choix de la personne effectuant les opérations de vote à distance.

Au cours des travaux que la commission a menés depuis 2003 et compte tenu des menaces qui pèsent sur ces dispositifs, 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 reste réservée quant à l'utilisation de dispositifs de vote par correspondance électronique, notamment via Internet, pour des élections politiques.
La présente délibération a pour objet de revoir la recommandation de 2010 à l'aune des opérations électorales intervenues depuis, de l'évolution des solutions de vote proposées par les prestataires du secteur, des retours effectués par les différentes parties prenantes, des contrôles réalisés par la CNIL ainsi que de l'évolution du cadre juridique relatif à la protection des données.

La nouvelle recommandation a pour champ d'application les dispositifs de vote par correspondance électronique, en particulier via Internet. Elle ne concerne pas les dispositifs de vote par codes-barres, les dispositifs de vote par téléphone fixe ou mobile, ni les systèmes informatiques mis à disposition des votants sous forme de boîtiers de vote ou en isoloirs (dites « machines à voter »). Elle est destinée à fixer, de façon pragmatique, les objectifs de sécurité que doit atteindre tout dispositif de vote par correspondance électronique, notamment via Internet, en fonction des risques que présente le déroulement du vote. Les réponses apportées par les systèmes à ces objectifs de sécurité doivent ainsi prendre en compte le contexte et les menaces qui pèsent sur le scrutin.

Elle vise également à s'appliquer aux futures évolutions des systèmes de vote par correspondance électronique, notamment via Internet, 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 par correspondance électronique à retenir.

Elle abroge la délibération n° 2010-371 du 21 octobre 2010 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. Le niveau de risque du scrutin.

Le niveau de risque que présente le déroulement d'un vote varie en fonction du type de scrutin, des évènements redoutés et des menaces qui pèsent sur le traitement.
Ainsi, la commission recommande que la solution utilisée pour le scrutin tienne compte de l'importance du niveau de risque de l'élection ainsi que des éventuels bénéfices pour les parties prenantes de recourir à un système de vote par correspondance électronique et que la solution choisie réponde à tous les objectifs de sécurité fixés au regard de ce niveau de risque.

La commission identifie trois niveaux de risque :

- **Niveau 1** : Les sources de menace, parmi les votants, les organisateurs du scrutin ou les personnes extérieures, ont peu de ressources et peu de motivations. L'administrateur (ou les administrateurs) du système d'information n'est ni électeur, ni candidat.
Il est considéré comme neutre par toutes les parties. Ce niveau s'applique pour les scrutins impliquant peu d'électeurs, se déroulant dans un cadre non conflictuel, à l'issue duquel les personnes élues auront peu de pouvoirs, comme par exemple l'élection d'un représentant de classe. Le scrutin ne présente pas de risques importants.

- **Niveau 2** : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources moyennes ou des motivations moyennes. Ce niveau s'applique à des scrutins impliquant un nombre important d'électeurs et présentant un enjeu élevé pour les personnes mais dans un contexte dépourvu de conflictualité particulière. Il s'agit par exemple des élections de représentants du personnel au sein d'organismes ou encore au sein d'un ordre professionnel. Le scrutin présente un risque modéré.

- **Niveau 3** : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources importantes ou de fortes motivations. Ce niveau concerne les scrutins impliquant un nombre important d'électeurs et présentant un enjeu très élevé, dans un climat potentiellement conflictuel.

Il s'agit par exemple d'élections de représentants du personnel au sein d'organisations importantes, à grande échelle et dans un cadre conflictuel. Le scrutin présente un risque important.
La commission déconseille d'utiliser un dispositif de vote par correspondance électronique, notamment via Internet, dans l'hypothèse où les sources de menace peuvent disposer à la fois de ressources
importantes et d'une motivation forte. Le responsable du traitement identifie le niveau correspondant à sa situation en fonction des risques soulevés par son scrutin.

A cette fin la commission propose, de manière facultative et à titre d'exemple, une grille d'analyse simplifiée, basée sur des questions fermées, ayant pour objet de guider et d'aider les responsables de traitement le désirant à se positionner sur cette échelle. Cette grille d'analyse est placée au sein de la fiche pratique.

En cas de doute entre deux niveaux, le niveau le plus élevé devrait être privilégié. Le responsable de traitement, maitrisant le périmètre, les enjeux et le contexte de son scrutin, est libre de choisir le niveau de risque qu'il juge approprié, dès lors qu'il peut justifier son analyse auprès de la commission et de l'expert indépendant.

Une fois son niveau de risque identifié, le responsable de traitement peut déterminer les objectifs de sécurité que la solution de vote doit atteindre.

Le choix du niveau de risque par le responsable de traitement étant évalué par l'expert indépendant mandaté (voir ci-après) pour garantir la conformité des opérations de vote à la présente recommandation, il convient que le responsable de traitement lui fournisse les éléments ayant été pris en compte dans la détermination de ce niveau.

D'une manière générale, la commission rappelle que les traitements de données personnelles, dont les dispositifs de vote, qui remplissent au moins deux des critères suivants doivent en principe faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) :

- évaluation/« *scoring* » (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles (opinions politiques et appartenances syndicales notamment) ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une technologie nouvelle) ;
- exclusion du bénéfice d'un droit/contrat.

Dès lors, au regard des critères relatifs aux données sensibles et à la collecte de données à large échelle et compte tenu du contexte du scrutin le cas échéant, il peut être nécessaire que le responsable de traitement réalise une AIPD.

Les objectifs de sécurité à atteindre en fonction du niveau de risque
Chaque niveau de risque se voit associer des objectifs de sécurité qui permettent de définir le niveau de sécurité attendu. Ces objectifs sont cumulables, le niveau 2 étant composé d'objectifs de sécurité spécifiques et des objectifs de sécurité du niveau 1, le niveau 3 étant, quant à lui, composé d'objectifs de sécurité spécifiques et des objectifs de sécurité des deux niveaux précédents.

La commission proposera sur son site web ou tout autre support utile, une fiche pratique présentant des exemples permettant d'atteindre les objectifs de sécurité précités. Les industriels peuvent, s'ils le souhaitent, proposer à la commission des exemples de moyens permettant d'atteindre les objectifs afin que cette fiche puisse être agrémentée de ces informations.

La commission sera seule juge de la pertinence des moyens proposés. Cette fiche détaillera ce qui est attendu derrière chaque objectif de sécurité.

Les solutions de vote dont le scrutin présente un risque de niveau 1 doivent atteindre a minima l'ensemble des objectifs de sécurité suivants :

- **Objectif de sécurité n° 1-01** : Mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers).
- **Objectif de sécurité n° 1-02** : Définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.
- **Objectif de sécurité n° 1-03** : Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduits de manière significative.
- **Objectif de sécurité n° 1-04** : Assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant.
- **Objectif de sécurité n° 1-05** : Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.
- **Objectif de sécurité n° 1-06** : Assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement.
- **Objectif de sécurité n° 1-07** : Assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement.
- **Objectif de sécurité n° 1-08** : Renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.
- **Objectif de sécurité n° 1-09** : Définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin.
- **Objectif de sécurité n° 1-10** : Assurer l'intégrité du système, de l'urne et de la liste d'émargement.
- **Objectif de sécurité n° 1-11** : S'assurer que le dépouillement de l'urne puisse être vérifié a posteriori. Les solutions de vote dont le scrutin présente un risque de niveau 2 doivent atteindre a minima l'ensemble des objectifs de sécurité du niveau 1 ainsi que les suivants :
- **Objectif de sécurité n° 2-01** : Assurer une haute disponibilité de la solution.
- **Objectif de sécurité n° 2-02** : Assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement.
- **Objectif de sécurité n° 2-03** : Permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin.
- **Objectif de sécurité n° 2-04** : Authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.
- **Objectif de sécurité n° 2-05** : Assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.
- **Objectif de sécurité n° 2-06** : Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.
- **Objectif de sécurité n° 2-07** : Assurer la transparence de l'urne pour tous les électeurs.

Les solutions de vote dont le scrutin présente un risque de niveau 3 doivent atteindre a minima l'ensemble des objectifs de sécurité des niveaux 1 et 2, ainsi que les suivants :
- **Objectif de sécurité n° 3-01** : Étudier les risques selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte de mise en œuvre.
- **Objectif de sécurité n° 3-02** : Permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers.
- **Objectif de sécurité n° 3-03** : Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.
- **Objectif de sécurité n° 3-04** : Permettre le contrôle automatique et manuel par le bureau électoral de l'intégrité de la plateforme pendant tout le scrutin.
- **Objectif de sécurité n° 3-05** : Assurer un cloisonnement physique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.

Le responsable de traitement ou son prestataire sont libres d'utiliser toute solution leur permettant d'atteindre les objectifs de sécurité énoncés.

Quel que soit le niveau déterminé, 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 par correspondance électronique, notamment via Internet. Cette notice explicative ne se substitue pas à l'obligation d'information imposée par les articles 13 et 14 du règlement européen sur la protection des données (RGPD) s'agissant du traitement des données.

Parallèlement, la commission tient à souligner que, de par leur nature et sensibilité, les plateformes de vote par correspondance électronique, notamment via Internet, se doivent d'être accessibles à toutes personnes, notamment aux personnes en situation de handicap et en particulier visuel.
Ainsi, pour les organismes du secteur public ou délégataires d'une mission de service public désirant proposer ce service à ses électeurs, il est nécessaire que le système de vote respecte le référentiel général d'accessibilité pour les administrations (RGAA).

Pour les organismes non soumis à ce référentiel, il est fortement recommandé d'en suivre les prescriptions afin de mettre l'ensemble des votants en capacité d'exprimer leur suffrage par ce moyen.
L'expertise du système de vote par correspondance électronique, notamment via Internet
Tout responsable de traitement mettant en œuvre un système de vote par correspondance électronique, notamment via Internet, doit faire expertiser sa solution par un expert indépendant, que la solution de vote soit gérée en interne ou fournie par un prestataire.

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

L'expertise doit porter sur l'ensemble des éléments décrits dans la présente délibération et notamment sur :
- le code source correspondant à la version du logiciel effectivement mise en œuvre ;
- les mécanismes de scellement utilisés aux différentes étapes du scrutin ;
- le système informatique sur lequel le vote va se dérouler ;
- les échanges réseau ;
- les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote ;
- les mécanismes d'authentification des électeurs et la transmission des secrets à ces derniers ;
- l'évaluation du niveau de risque du scrutin ;
- la pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité.

L'expertise doit porter sur l'ensemble des éléments constituant la solution de vote.
Lors de scrutins présentant un niveau de risque 2 ou 3, l'expert réalise des audits sur la plateforme, afin de s'assurer de la cohérence et de l'effectivité des solutions apportées, par le biais de tests d'intrusions notamment. L'ensemble des opérations effectuées dans ce cadre est annexé au rapport d'expertise.
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 dans la société qui a créé la solution de vote à expertiser, ni dans l'organisme responsable de traitement qui a décidé d'utiliser la solution de vote ;
- posséder si possible une expérience dans l'analyse des systèmes de vote, en ayant expertisé les systèmes de vote par correspondance électronique, notamment via Internet, d'au moins deux prestataires différents.
Le rapport d'expertise, et ses annexes doivent être remis au responsable de traitement et aux prestataires de solution de vote par correspondance électronique, notamment via Internet.
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. Pour ce faire, l'expert peut, par exemple, utiliser des empreintes numériques.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 1 peut reprendre des éléments d'un rapport d'expertise précédent, dès lors que cette expertise effectuée sur l'élément en question n'est pas antérieure à 24 mois, qu'il est possible de prouver que l'élément sur lequel a porté cette expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont niveau de risque évalué à 3 doit être réalisée de nouveau, pour chaque élément, pour chaque élection.
L'expert ayant accès à des informations sensibles relatives aux solutions dont il est chargé d'évaluer la conformité, notamment le code source des applications, il est tenu de prendre toutes dispositions et précautions utilises afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source au sein du rapport, en conservant ses rapports au sein d'espaces sécurisés dédiés et en ne conservant pas les éléments portés à sa connaissance au-delà de la durée nécessaire.

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.

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

Pour se connecter à distance ou sur place au système de vote, l'électeur doit s'authentifier conformément à la présente recommandation et à l'aide d'un moyen répondant à l'objectif de sécurité correspondant au niveau de risque identifié pour le scrutin. 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.

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 reçoit alors la confirmation de son vote et dispose de la possibilité de conserver trace de cette confirmation.

La solution de vote par correspondance électronique, notamment via Internet, doit proposer toutes les options offertes par les textes fondant le vote, le cas échéant le vote nul ou blanc.

Dans le cas où le scrutin est mixte, composé d'un vote par correspondance électronique associé à un vote par correspondance papier par exemple, il convient que le vote électronique permette aux électeurs les mêmes possibilités que celles offertes par le vote papier, telle que la possibilité de voter nul ou blanc lorsque cela est prévu pour un scrutin, afin de ne pas créer de distorsion en fonction du moyen utilisé. Dans le cas où ces différentes possibilités sont offertes à l'électeur, il convient d'être attentif au fait qu'une personne ne puisse pas voter deux fois, notamment en utilisant le système par correspondance papier et le système par Internet.
Ainsi la solution retenue doit permettre d'écarter les votes par correspondance papier d'une personne ayant déjà voté par Internet.

Les garanties minimales pour un contrôle a posteriori pour des besoins d'audit externe, notamment en cas de contentieux électoral, le système de vote par correspondance électronique, notamment via Internet, doit pouvoir 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 détenteurs ;
- le vote est anonyme lorsque la législation l'impose ;
- la liste d'émargement ne comprend que la liste des électeurs ayant voté ;
- l'urne dépouillée est bien celle contenant les suffrages des électeurs et qu'elle ne contient que ces suffrages ;
- aucun décompte partiel n'a pu être effectué durant le scrutin ;
- le dépouillement de l'urne peut être vérifié a posteriori et qu'il s'est déroulé de façon correcte.

La conservation des données portant sur l'opération électorale
Tous les fichiers supports (copies des codes sources et exécutables des programmes et du système sous- jacent, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) doivent être conservés sous scellés jusqu'à l'épuisement des voies et 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 au prestataire de service, le cas échéant, de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation de ces supports. Lorsqu'aucune action contentieuse n'a été engagée à l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.
Dispositions transitoires et finales
La présente délibération est publiée au Journal officiel de la République française. Elle devra être prise en compte par les responsables de traitement après un délai transitoire de douze mois à compter de sa publication.

La présidente,
M.-L. Denis

ANNEXE III

Scrutin de liste à un tour avec représentation proportionnelle au plus fort reste

Le calcul du quotient électoral est le rapport du nombre de suffrages exprimés à celui de sièges à pourvoir. Chaque liste obtient autant de sièges que le quotient électoral est contenu dans le nombre de suffrages.

S'il y a des sièges encore non attribués, ceux-ci sont, dans un deuxième temps réparti entre toutes les listes par valeur décroissante des restes.

L'exemple suivant illustre cette méthode :

- Inscrits : 3 784
- Votants : 1 342
- Nuls, blancs : 31
- Exprimés : 1 311

Quotient électoral Sièges à pourvoir : 3 1 311/3 = 437

Listes
A : 510 voix
B : 241 voix
C : 560 voix

Attribution des sièges
1er siège revient à la liste C pour laquelle il reste 123 voix
Le 2ème siège revient à la liste A pour laquelle il reste
73 voix Le 3ème siège à pourvoir revient à la liste B