

11

**ACCORD COLLECTIF RELATIF AUX CONDITIONS ET AUX MODALITES DE VOTE PAR VOIE  
ELECTRONIQUE POUR L'ELECTION  
DU REPRESENTANT FRANÇAIS AU CONSEIL DE SURVEILLANCE  
DE LA SOCIETE EUROPEENNE SAP SE**

**ENTRE LES SOUSSIGNES :**

La **Société SAP FRANCE S.A.**, dont le siège social est situé à Levallois-Perret (92300) - 35, rue d'Alsace, immatriculée au Registre du Commerce et des Sociétés de Nanterre sous le numéro 379 821 994, représentée par Madame Valérie VEZINHET en sa qualité de DRH Groupe SAP France et Madame Emmanuelle BRUN NECKEBROCK en sa qualité de Directeur Général Délégué.

La **Société SAP FRANCE HOLDING S.A.**, dont le siège social est situé à Levallois-Perret (92300) - 35, rue d'Alsace, immatriculée au Registre du Commerce et des Sociétés de Nanterre sous le numéro 341 612 687, représentée par Madame Valérie VEZINHET en sa qualité de DRH Groupe SAP France et Madame Emmanuelle BRUN NECKEBROCK en sa qualité de « Délégué » de Monsieur Franck COHEN Directeur Général.

Constituant ensemble une Unité Economique et Sociale, dénommée ci-après l'UES SAP,

**D'UNE PART**

**ET**

Les organisations syndicales représentatives au niveau de l'UES SAP, représentées par leurs délégués syndicaux.

**D'AUTRE PART**

(ci-après dénommées ensemble "les parties")

W<sub>1</sub> <sup>33</sup>  
RW  
PN

## **PREAMBULE**

Il est rappelé que

L'UES SAP est constituée d'établissements principaux et secondaires répartis sur l'ensemble du territoire français.

Par ailleurs, la majorité de l'électorat est constitué de salariés dont les fonctions les conduisent à effectuer des déplacements ponctuels et multiples voire des déplacements continus.

Dans ce cadre et pour faciliter l'organisation de l'élection du représentant des salariés au conseil de surveillance de la Société Européenne SAP SE et de son éventuel remplaçant, la Direction de l'UES SAP et les partenaires sociaux ont étudié les modalités proposées par la loi pour la Confiance dans l'Economie Numérique dite "loi Fontaine" qui ouvre la possibilité pour les entreprises de recourir au vote électronique pour les élections.

## **CECI ETANT EXPOSE, IL A ETE CONVENU CE QUI SUIT**

### **ARTICLE 1 : Etapes préalables à l'organisation de l'élection**

#### **1. Choix du prestataire**

Afin de garantir la sécurité des opérations électorales et la confidentialité du vote, les parties conviennent que l'élection sera organisée par le prestataire mandaté par la Direction parmi les trois suivants : « e-votez.com » ; « gedicom.fr » et « jevoteenligne.com » et après appel d'offres et ce dans le respect des dispositions énoncées aux articles R. 2314-8 et suivant du Code du travail.

#### **2. Dépôt de l'accord collectif**

Les parties rappellent que les formalités de dépôt de l'accord auprès de la Direction Départementale du Travail et de l'emploi compétente devront être réalisées au plus tard la veille de la signature du Protocole d'accord préélectoral (ci-après "PAP").

#### **3. Protocole d'accord préélectoral**

Dans le cadre de la présente élection, les organisations syndicales représentatives au niveau de l'UES SAP et la Direction signeront un PAP définissant notamment le calendrier et les modalités opératoires.

Le présent accord sera annexé au PAP. Celui-ci mentionnera en outre les noms du prestataire et de l'expert mandatés.

W  
2  
PN

#### 4. Déclaration CNIL

Les organisations syndicales de salariés représentatives dans le périmètre de l'accord seront tenues informées par la Direction de l'accomplissement des formalités déclaratives préalables auprès de la Commission Nationale de l'Informatique et des Libertés (ci-après "CNIL").

#### 5. Formation et informations sur le système de vote électronique du personnel

Les représentants du personnel, les délégués syndicaux, les membres du bureau de vote, les scrutateurs, les candidats et leurs représentants se verront offrir la possibilité de bénéficier d'une formation sur le système de vote électronique retenu. Le prestataire mettra à leur disposition tous documents utiles.

#### 6. Expertise indépendante

Le système de vote électronique, préalablement à sa mise en place ou à toute modification substantielle de sa conception, sera soumis à une expertise indépendante, destinée à vérifier le respect des prescriptions légales énoncées ci-dessus. Le rapport de l'expert sera tenu à la disposition de la CNIL ainsi que des instances représentatives du personnel et des organisations syndicales représentatives.

Les parties conviennent que l'expert mandaté sera le premier disponible sur la liste des experts judiciaires près la cour d'Appel de Versailles (réf ; E-01.04 Systèmes d'information – mise en œuvre).

#### 7. Mise en place de la cellule d'assistance technique

Une cellule d'assistance technique, composée de représentants de l'UES et le cas échéant, de représentants du prestataire mandaté, chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique sera mise en place.

En présence des candidats ou de leurs représentants, la cellule d'assistance technique :

1° Procèdera, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifiera que l'urne électronique est vide, scellée et chiffrée par au minimum 3 clés délivrées à cet effet ;

2° Procèdera, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement à l'issue duquel le système est scellé ;

3° Contrôlera, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système.

#### ARTICLE 2 : Préparation de l'élection

Les parties signataires adoptent un processus de vote par Internet à l'occasion de l'élection du représentant des salariés au conseil de surveillance de la Société Européenne SAP SE.

W  
3<sup>3</sup> RW  
PN

### 1. Etablissement des listes électorales

A des fins de préparation de l'élection, il sera établi un dossier nommé "fichier électeur", mis en place à partir de la liste électorale et qui sera transmis au prestataire choisi.

La liste électorale susmentionnée précise notamment les données suivantes : noms et prénoms des inscrits, date d'entrée dans l'entreprise et date de naissance.

Le "fichier électeur" a pour fin de délivrer à chaque électeur un moyen d'authentification qui lui permettra :

- ✓ de prendre part au vote ;
- ✓ d'être identifié et reconnu.

En outre, le "fichier électeur" permet d'éditer les listes d'émargements.

Le fichier dénommé "contenu de l'urne électronique" recense les votes exprimés par voie électronique. Les données de ce fichier font l'objet d'un chiffrement et ne doivent pas comporter de lien permettant l'identification des électeurs afin de garantir la confidentialité du vote.

### 2. Lieu et temps du scrutin

Afin d'assurer un taux de participation optimum, les parties conviennent, tant pour le premier tour que pour un éventuel second tour de scrutin, que l'élection aura lieu sur 4 jours le dernier jour étant ouvert pendant une période délimitée, et ce conformément au calendrier défini par le PAP.

Les dates et heures d'ouverture et de fermeture des scrutins seront indiquées dans le PAP.

Les électeurs auront la possibilité de voter à tout moment pendant la période d'ouverture du scrutin en se connectant au système de 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 à assurer le contrôle des opérations électorales.

Le système de vote électronique sera scellé à l'ouverture et à la clôture du scrutin.

### 3. Bulletins de vote électronique

Le système de vote électronique reproduit sur le serveur les candidatures telles qu'elles ont été présentées par leurs auteurs. Celles-ci apparaissent simultanément sur l'écran dans l'ordre alphabétique des sigles des organisations syndicales ou du nom patronymique du candidat titulaire présenté par 1/20<sup>ème</sup> des électeurs. En cas d'impossibilité de présentation simultanée sur l'écran, un tirage au sort détermine l'ordre d'apparition.

Dans l'éventualité d'un second tour, cet ordre reste inchangé.

W ✓  
R W  
P N

Par ailleurs, afin de ne pas favoriser une candidature plutôt qu'une autre, la dimension des bulletins, les caractères et la police utilisés sont d'un type uniforme pour toutes les listes.

Chaque bulletin devra comporter la mention « titulaire » et l'indication des noms et prénoms du candidat, la mention « remplaçant » avec l'indication des noms et prénoms de l'éventuel candidat et le titre éventuel de la candidature.

### **ARTICLE 3 : Déroulement des opérations de vote**

#### **1. Accès au serveur de vote électronique**

Avant le premier tour des élections, chaque électeur recevra, selon les modalités déterminées dans le cadre du PAP, ses codes d'accès générés de manière aléatoire.

A l'aide de ses identifiants personnels, l'électeur pourra voter en toute confidentialité en se connectant sur le site sécurisé des élections.

L'identification de l'électeur sera assurée par un serveur dédié, après saisie par l'utilisateur de ses codes d'accès. Toute personne non reconnue n'aura pas accès aux pages du serveur de vote.

Une fois connecté, l'électeur se verra présenter les bulletins correspondants.

La seule connexion au serveur ne vaudra pas vote.

Seule la validation par l'électeur de son vote vaudra vote, émargement avec horodatage et clôturera définitivement l'accès à cette élection. L'électeur recevra immédiatement confirmation de son vote et aura la possibilité de conserver une trace de cette confirmation.

**Consultation du nombre de votants** : pendant le déroulement du vote, aucun résultat partiel n'est accessible. Cependant, le nombre de votants peut être révélé au cours du scrutin, à la demande d'une organisation syndicale représentative, d'un candidat ou d'un de ses représentants ou d'une société entrant dans le périmètre de l'UES SAP

Pendant le déroulement du vote, au matin de chaque jour suivant le premier jour de vote, le prestataire remettra à l'employeur la mesure du taux de participation enregistré en précisant la date et l'heure de la mesure. L'employeur diffusera dans les meilleurs délais cette information à tous les salariés.

#### **2. Clôture et Résultats**

Dès la clôture du scrutin, le contenu de l'urne, les listes d'émargements et les états courants gérés par les serveurs seront figés, horodatés et scellés automatiquement sur l'ensemble des serveurs.

W  
3<sup>s</sup> RW  
PD

#### **ARTICLE 4 : Dispositions communes**

##### **1. Durée de l'accord**

Le présent accord est conclu pour la durée de l'élection 2015 du représentant des salariés au conseil de surveillance de la Société Européenne SAP SE.

##### **2. Révision - Dénonciation**

Le présent accord pourra être dénoncé à tout moment par l'une ou l'autre des parties signataires, sous réserve d'un délai de préavis de 3 mois. Cependant, une dénonciation ne pourra intervenir moins de 2 mois précédant l'élection du représentant des salariés au conseil de surveillance de la Société Européenne SAP SE.

Chacune des parties peut demander la révision de tout ou partie du présent accord, par lettre recommandée avec accusé de réception adressée à toutes les autres parties signataires, accompagnée de la nouvelle rédaction proposée. Cet accord de révision ne peut être conclu et signé que par les syndicats signataires de l'accord initial et par ceux qui ont éventuellement adhéré au texte.

La demande sera notifiée par lettre recommandée avec accusé de réception à tous les signataires des présentes.

##### **3. Dépôt et publicité**

Un exemplaire original de cet accord est remis à chacune des parties signataires.

Le présent accord sera affiché et communiqué à l'ensemble du Personnel.

Deux exemplaires originaux seront déposés par la partie la plus diligente auprès de la Direction Départementale du Travail et de l'emploi des Hauts de Seine et un exemplaire original sera déposé au secrétariat greffe du Conseil de Prud'hommes de NANTERRE.

Les formalités de dépôt seront également effectuées auprès des directions départementales du travail et de l'emploi, ainsi qu'au secrétariat greffe des Conseils de Prud'hommes dont relèvent les établissements des sociétés entrant dans le périmètre de l'UES SAP (cf. Annexe 2).

En outre, conformément à l'accord nationale du 15 septembre 2005 (Convention Collective Nationale des Bureaux d'Etudes Techniques, Cabinets d'Ingénieurs Conseils et Sociétés de Conseils), un exemplaire sera remis à l'Observatoire Paritaire de la Négociation Collective.

W ✓  
ES  
" RW  
PN


Fait à Levallois, le 4 décembre 2014.

Pour l'UES SAP France

**Valérie VEZINHET**  
Directrice des Ressources Humaines  
SAP France  
Dûment habilitée



**Emmanuelle BRUN-NECKEBROCK**  
Déléгатaire de Monsieur COHEN  
Directeur Général de SAP France Holding  
Directeur Général Délégué SAP France  
Dûment habilitée



le 01/12/2014

Pour la CFE-CGC SNEPSSI

Dûment habilité



Pour la Fédération CGT  
Des Sociétés d'Etudes

Dûment habilité

Pour la CFDT-F3C

**Rémy CHAMBARD-WILLIAMS**  
Dûment habilité



Raw  
PA

## ANNEXE 1 - CAHIER DES CHARGES

La délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique fait partie intégrante du présent cahier des charges.

En outre :

Le dispositif de vote électronique respecte les principes généraux du droit électoral et permet d'assurer l'identité des électeurs, la sincérité et le secret du vote, ainsi que la publicité du scrutin.

### ARTICLE 1 : Confidentialité des données transmises

Le dispositif assure la confidentialité des données transmises, à savoir :

- ✓ les fichiers constitués pour établir les listes électorales des collèges électoraux ;
- ✓ la sécurité de l'adressage des moyens d'authentification ;
- ✓ l'émargement ;
- ✓ l'enregistrement et le dépouillement des votes.

Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne sont uniquement accessibles aux personnes chargées de la gestion et de la maintenance du système.

Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote sont traitées par des systèmes informatiques distincts, dédiés et isolés : ces fichiers sont respectivement dénommés « fichier des électeurs » et « contenu de l'urne électronique ».

Le système de vote électronique est conçu de manière à pouvoir être scellé à l'ouverture et à la clôture du scrutin.

### ARTICLE 2 : Contenu des fichiers

Le « fichier des électeurs », établi à partir des listes électorales permet de délivrer à chaque électeur un moyen d'authentification, d'identifier les électeurs ayant voté et d'éditer les listes d'émargement.

Le fichier « contenu de l'urne électronique » recense pour sa part les votes exprimés par voie électronique.

Les données enregistrées sont :

- ✓ **listes électorales** : nom et prénom des inscrits, date d'entrée dans l'entreprise, date de naissance, collège électoral ;

W<sup>B</sup> RW<sup>CS</sup>

PR



- ✓ **fichier des électeurs** : noms et prénoms, collège électoral, moyen d'authentification et coordonnées, le cas échéant ;
- ✓ **listes d'émargement** : collège électoral, nom et prénom des électeurs ;
- ✓ **candidatures** : collège électoral, nom et prénom des candidats, titulaires et remplaçants, appartenance syndicale ;
- ✓ **listes de résultats** : nom et prénom des candidats, élus, non élus, voix obtenues, appartenance syndicale, collège et destinataires.

Les destinataires des données sont :

- ✓ **pour les listes électorales** : les électeurs, les syndicats représentatifs, les agents habilités des services du personnel ;
- ✓ **pour le fichier des électeurs** : les électeurs, pour les informations qui les concernent ;
- ✓ **pour les listes d'émargement** : les membres des bureaux de vote, les agents habilités des services du personnel ;
- ✓ **pour les candidatures** : les électeurs, les syndicats, les agents habilités des services du personnel ;
- ✓ **pour les listes des résultats** : les électeurs, les services du ministère chargé de l'emploi, les syndicats, l'employeur ou les agents habilités des services du personnel.

### ARTICLE 3 : Garantie des exigences techniques

Afin de s'assurer du respect des exigences techniques du dispositif, le dispositif de vote électronique doit être, préalablement à sa mise en place, soumis à une expertise indépendante, afin de vérifier le respect des prescriptions légales et réglementaire. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Les personnes chargées de la gestion et de la maintenance du système informatique doivent toujours s'assurer du respect des prescriptions légales et réglementaires.

Un dispositif de secours offrant les mêmes garanties que le dispositif principal, est mis en place pour prendre le relais en cas de panne du système.

### ARTICLE 4 : Mise en place d'une cellule d'assistance technique

Une cellule d'assistance technique, composée de représentants de l'UES et le cas échéant, de représentants du prestataire mandaté, chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique sera mise en place.

En présence des candidats ou de leurs représentants, la cellule d'assistance technique :

W  
3  
9 RW  
PN

1° Procèdera, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifiera que l'urne électronique est vide, scellée et chiffrée par au minimum 3 clés délivrées à cet effet ;

2° Procèdera, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement à l'issue duquel le système est scellé ;

3° Contrôlera, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système.

#### **ARTICLE 5 : Déroulement du vote**

La dimension des bulletins électroniques, les caractères et la police utilisés doivent être identiques pour toutes les listes.

Le choix de l'électeur doit clairement apparaître à l'écran.

L'électeur doit pouvoir modifier son choix avant validation.

La validation entraînant transmission du vote et émargement fait l'objet d'un accusé de réception que l'électeur doit pouvoir conserver.

#### **ARTICLE 6 : Dépouillement**

A la clôture des opérations de vote, la cellule d'assistance technique vérifie le scellement du système.

L'ensemble des données est alors figé, horodaté et scellé.

L'accès aux données du fichier « contenu de l'urne électronique » ne peut se faire que par activation conjointe, par deux clés de chiffrement détenues par le Président et les assesseurs.

Les données sont conservées sous scellés jusqu'à l'expiration du délai de recours (15 jours en matière d'élections professionnelles) ou, en cas d'action contentieuse, jusqu'à ce que la décision de justice acquière caractère définitif. Elles peuvent ensuite être détruites.

W ✓ 10 05  
KW  
PP

**ANNEXE 2 - LISTE DES ETABLISSEMENTS PRINCIPAUX ET SECONDAIRES DE L'UES SAP**

**AU 1ER NOVEMBRE 2014**

**SAP France HOLDING**

Etablissement principal :

35 rue d'Alsace, 92300 Levallois-Perret

Autre établissement :

23/25 rue Delarivière Lefoullon Tour Défense Plaza 92800 Puteaux

**SAP France**

Etablissement principal :

35 rue d'Alsace – 92300 Levallois-Perret

Autres établissements :

157 – 159 rue Anatole France – 92300 Levallois-Perret

23/25 rue Delarivière Lefoullon – Défense Plaza – La Défense 9 – 92064 Paris La Défense  
CEDEX

15/17 rue Pagès – 92150 Suresnes

RCS Aix-en-Provence

R.C.S Toulouse

R.C.S Bordeaux

R.C.S Nantes

R.C.S Strasbourg

R.C.S Lyon

W  
M " PAW  
PA

R.C.S Paris

✓✓<sup>12</sup>  
KW  
PA

**ANNEXE 3 – DELIBERATION N° 2010-371 DU 21 OCTOBRE 2010 PORTANT ADOPTION  
D'UNE RECOMMANDATION RELATIVE A LA SECURITE DES SYSTEMES DE VOTE  
ELECTRONIQUE**

W  
3 13 RW  
PA

W ✓  
CS  
Rau  
PR

## Commission nationale de l'informatique et des libertés

### Délibération n° 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 n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

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

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 n° 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 n° 2003-036 du 1<sup>er</sup> 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 :

W RW  
in PD

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.

W  
 5 RW  
 PN



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

VW  
RW  
BS  
PA

— —

100

\*

✓✓

ES RW  
PP