Recommandation

relative à la sécurité des systèmes de vote par correspondance électronique

Adoptée le 19 mars 2026

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Portée de la recommandation

1. La présente recommandation remplace les dispositions de la recommandation du 25 avril 2019. Elle prend en compte les opérations électorales intervenues depuis, l'évolution des systèmes de vote proposés par les prestataires du secteur, les retours effectués par différentes parties prenantes à des opérations de vote par correspondance électronique, ainsi que les contrôles réalisés par la CNIL.

2. Cette mise à jour s'inscrit dans la cadre d'une collaboration avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

3. Cette recommandation fixe, de façon concrète, les objectifs de sécurité minimaux que devraient atteindre les dispositifs de vote par correspondance électronique utilisés pour la mise en œuvre d'un vote à bulletin secret, en fonction des risques que présentent l'organisation et le déroulement du vote. Les réponses apportées à ces objectifs de sécurité doivent prendre en compte le contexte et les menaces spécifiques qui pèsent sur chaque scrutin.

4. Sont exclus de son champ d'application les dispositifs de vote par codes-barres, les dispositifs de vote par SMS ou appel téléphonique et les systèmes informatiques mis à disposition des votants sous forme de boîtiers de vote ou de machines à voter, ainsi que les scrutins non-secrets.

5. Cette recommandation est applicable aux solutions de vote par correspondance électronique utilisées dans le cadre de scrutins à bulletin secret combinant plusieurs modalités de vote. Il appartient dans ce cas aux organisateurs du scrutin de s'assurer que le choix des modalités retenues ne permet pas de compromettre les principes fondamentaux que doit garantir la solution de vote électronique.

6. La recommandation vise en particulier :
   - à favoriser l'évolution des systèmes de vote par correspondance électronique en vue d'un meilleur respect des principes généraux du droit électoral et de la protection des données personnelles ; elle s'adresse donc notamment aux fournisseurs de ces systèmes ;
   - à éclairer les organisateurs de scrutins dans leurs choix de systèmes de vote adaptés à leurs scrutins.

7. Elle s'adresse par ailleurs aux personnes en charge de l'audit des solutions de vote électronique afin de les aider à en évaluer la conformité.

2. Principes fondamentaux applicables aux opérations de vote par correspondance électronique dans le cadre de scrutins à bulletin secret

8. La CNIL rappelle que **le recours au vote par correspondance électronique doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales concernées.** Elle propose ci-dessous une traduction de ces

principes en objectifs à atteindre, desquels résultent des recommandations et objectifs de sécurité proposés dans ce document :

- le **secret du scrutin** : aucun lien ne doit pouvoir être établi entre un votant et l'expression de son vote (c'est-à-dire le contenu de son bulletin), afin de garantir, d'une part, la confidentialité du choix réalisé par le votant, et d'autre part, l'anonymat du vote, afin de limiter le risque d'intimidation, de manipulation ou de corruption des votants ;
- le **caractère personnel du vote** : le risque de recours abusif à la délégation de vote, et donc à l'achat de vote, ainsi que le risque d'usurpation d'identité doivent pouvoir être limités ;
- le **caractère libre du vote** : les membres du corps électoral doivent être à l'abri de toute pression, et les parties prenantes à l'organisation de l'élection doivent être neutres et objectives, garantissant notamment l'égalité entre les candidats. Le respect de ce principe peut dépendre de facteurs extérieurs au système de vote par correspondance électronique ;
- la **sincérité des opérations électorales** : le vote ne doit être accessible qu'aux électeurs inscrits sur les listes électorales, et le résultat des opérations de vote doit représenter la volonté exprimée des votants ;
- l'**intégrité des suffrages exprimés** : le choix d'un électeur ne doit pas pouvoir être modifié entre son émission et sa prise en compte au moment du décompte des suffrages.
- l'**accès au vote pour tous les électeurs** : l'organisation des opérations électorales doit permettre à chaque électeur d'exprimer son vote ;
- la **surveillance effective du vote** : l'organisation, le déroulement et le dépouillement des opérations électorales doivent faire l'objet d'un contrôle régulier, indépendant et objectif ;
- la possibilité de **contrôle *a posteriori* de l'élection par un juge** : en cas de contestation du résultat du scrutin, un juge électoral doit pouvoir déterminer si des irrégularités ont affecté le déroulement des opérations électorales.

9. La CNIL observe que le respect de ces principes fondamentaux dans le contexte du vote par correspondance électronique – tout comme lors du recours au vote postal – fait peser des exigences élevées sur les personnes chargées d'organiser le scrutin et celles chargées d'en vérifier le déroulement. Ces exigences découlent notamment de la complexité et de l'opacité techniques de la plupart des systèmes de vote électronique, ainsi que de la très grande difficulté de s'assurer de la réelle identité et de la liberté de choix des personnes effectuant les opérations de vote à distance.

10. Au cours de ses travaux menés depuis 2003, la CNIL a constaté que les systèmes de vote par correspondance électronique ne semblent pas en mesure de fournir simultanément et au plus haut niveau l'ensemble des garanties exigibles par les textes légaux (une exigence forte sur la sincérité des opérations électorales pouvant par exemple diminuer le niveau de secret du scrutin). De plus, le contexte actuel, marqué par l'intensification des risques cyber et des opérations d'ingérence étrangères, appelle à une vigilance accrue. Dès lors, **la CNIL reste très réservée quant à l'utilisation de dispositifs de vote par correspondance électronique pour des scrutins politiques**, notamment lorsque ces scrutins peuvent être organisés en présentiel. La CNIL entend par « scrutins politiques » les scrutins locaux, nationaux et européens ayant pour but soit de désigner des responsables politiques, soit de consulter les électeurs sur des projets de résolutions ou de textes (référendums). À ce jour, la loi française limite le vote électronique pour les scrutins politiques aux votes des Français

résidant à l'étranger pour les élections législatives et les élections des conseillers des français de l'étranger (qui représentent les Français de l'étranger auprès des ambassades et des consulats). La CNIL estime qu'il convient d'appliquer *a minima* à ces scrutins ses recommandations correspondant au niveau de risque le plus élevé.

11. Compte tenu de ces observations préalables, la CNIL émet la recommandation suivante.

3. Typologie des niveaux de risque applicables aux scrutins

12. Le niveau de risque que présentent l'organisation et le déroulement d'un vote par correspondance électronique varie en fonction du type de scrutin, du contexte dans lequel il est organisé, des événements redoutés et des menaces qui pèsent sur le traitement.

13. L'analyse de ces facteurs ne doit pas se limiter à l'appréciation de l'impact potentiel des atteintes à la sécurité du système de vote électronique (« SVE ») sur les principes fondamentaux du droit électoral rappelés précédemment mais doit également s'intéresser au respect de l'ensemble des obligations découlant du traitement des données personnelles des électeurs.

14. À titre d'exemple, un accès non-autorisé au fichier des électeurs peut constituer une violation de données au sens du RGPD et porter atteinte aux droits des votants, alors même qu'il pourrait ne pas avoir d'impact avéré sur la sincérité ou sur le secret des opérations de vote.

15. Les facteurs humains et organisationnels, tels que le temps et les moyens disponibles pour l'organisation de l'élection, l'expérience des équipes concernées et les caractéristiques des électeurs (notamment leurs compétences numériques), devraient également être pris en compte.

16. La CNIL recommande que le choix de recourir au vote par correspondance électronique, en remplacement ou en complément du vote à l'urne ou du vote postal, tienne compte du niveau de risque du scrutin au regard des éventuels bénéfices pour les parties prenantes (en particulier lorsque que la difficulté d'accès au scrutin pour les électeurs entraine une abstention importante). Elle recommande que la solution de vote électronique mise en œuvre réponde à tous les objectifs de sécurité correspondant au niveau de risque du scrutin.

17. La recommandation de la CNIL entend à cet égard couvrir les trois niveaux de risque définis ci-dessous :

- **Niveau 1** (risques faibles) : les sources de menace (parmi les votants, les organisateurs du scrutin, les fournisseurs du système de vote, les personnes extérieures, etc.) ont peu de ressources et peu de motivations. L'administrateur (ou les administrateurs) du système d'information n'est ni votant, ni candidat. Il est considéré comme neutre par toutes les parties.

  Ce niveau s'applique principalement pour les scrutins qui impliquent un faible nombre de votants, qui se déroulent dans un cadre non conflictuel, qui ne révèlent ni les orientations politiques, ni les opinions syndicales des personnes, et à l'issue desquels les personnes élues auront, le cas échéant, peu de pouvoirs.

Il peut par exemple s'agir d'élections de représentants de parents d'élèves dans les établissements scolaires ou de scrutins organisés au sein d'associations locales.

- **Niveau 2** (risques modérés) : les sources de menace (parmi les votants, les organisateurs du scrutin, les fournisseurs du système de vote, les personnes extérieures, etc.) peuvent disposer de ressources moyennes et de motivations moyennes.

  Ce niveau s'applique principalement à des scrutins qui impliquent un nombre modéré de votants et qui présentent un enjeu moyen pour les candidats dans un contexte dépourvu de conflictualité particulière.

  Il s'agit par exemple des élections de représentants du personnel au sein d'organismes de petite taille ou de taille moyenne.

- **Niveau 3** (risques significatifs) : les sources de menace (parmi les votants, les organisateurs du scrutin, les fournisseurs du système de vote, les personnes extérieures, etc.) peuvent disposer de ressources importantes ou de fortes motivations.

  Ce niveau concerne principalement les scrutins qui impliquent un nombre de votants important et qui présentent un enjeu élevé pour les candidats ou se déroulent dans un climat potentiellement conflictuel.

  Il peut par exemple s'agir d'élections organisées au sein d'ordres professionnels réglementés, des primaires de partis politiques, ou d'élections de représentants du personnel au sein d'organisations importantes.

18. La CNIL déconseille de recourir au vote par correspondance électronique dans l'hypothèse où les sources de menace peuvent disposer à la fois de ressources importantes et d'une motivation forte, par exemple si des risques d'ingérence étrangère sont identifiés. Elle considère en effet que les solutions envisageables à ce jour ne permettent pas de se prémunir du niveau de risque très élevé qui en découlerait.

4. Évaluation du niveau de risque d'un scrutin

19. L'organisateur du scrutin identifie le niveau correspondant à sa situation en fonction des risques organisationnels et techniques soulevés par son scrutin. À cette fin la CNIL propose la grille d'analyse simplifiée ci-après. Cette grille a pour objet d'aider l'organisateur du scrutin à positionner un scrutin sur l'échelle de niveaux de risque précédemment détaillée. Son usage est facultatif et elle n'a pas vocation à se substituer à une analyse approfondie et tenant compte de tous les éléments de contexte pertinents.

Questions valant 1 point (en cas de réponse positive)	Oui	Non
Question 1 : Le scrutin concerne-t-il plus de 250 personnes ?		
Question 2 : Le scrutin concerne-t-il plus de 2 000 personnes ?		
Question 3 : L'entité organisatrice des élections a-t-elle déjà été victime d'attaques informatiques (avec ou sans lien avec des élections) dans les cinq dernières années ?		
Question 4 : Durant les cinq dernières années, les résultats d'un ou de certains scrutins similaires ont-ils été contestés devant une juridiction ?		
Question 5 : Certaines personnes directement intéressées par le résultat du scrutin pourraient-elles avoir accès aux données nécessaires à la mise en œuvre de la procédure de renouvellement d'accès des électeurs au SVE ?		
Question 6 : Une atteinte à la confidentialité du scrutin serait-t-elle de nature à révéler les opinions politiques, les convictions philosophiques ou l'appartenance syndicale des électeurs ?		
Question 7 : L'organisme RT est-il une entité importante ou essentielle au sens de la directive NIS2[1] ?		
Question 8 : La liste des électeurs ou les données utilisées pour l'accès ou le renouvellement d'accès de ceux-ci présentent-t-elles un intérêt en soi pour un attaquant (puissance étrangère, acteur malveillant, etc.) ?		
Question 9 : Les instances ou les personnes élues à l'issue du scrutin jouissent-elles d'un statut protecteur, tel que la protection contre le licenciement par exemple ?		
Question 10 : Les instances ou les personnes élues à l'issue du scrutin disposent-elles de pouvoirs organisationnels ou financiers ?		
Question 11 : L'organisation du scrutin constitue-t-elle la première mise en œuvre d'une solution de vote électronique par l'organisateur du scrutin ?		
Questions valant 2 points (en cas de réponse positive)	**Oui**	**Non**
Question 12 : Les instances ou les personnes élues à l'issue du scrutin disposent-elles de pouvoirs de sanction à l'égard de tiers ?		
Question 13 : Le scrutin permet-il la désignation de candidats à une élection « politique » (cas des primaires de partis politiques par exemple) ?		
Question 14 : L'organisation du scrutin risque-elle de nécessiter des développements techniques spécifiques importants ?		
Total		

[1] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE)

20. Une fois cette grille d'analyse complétée, l'organisateur du scrutin compte le nombre de questions pour lesquelles il a inscrit la réponse « oui », les trois dernières questions valant chacune 2 points. Le score obtenu permet de réaliser une première évaluation, indicative, du niveau de risque du scrutin :

    - entre 0 et 4 points : le risque est évalué au niveau 1 (risques faibles) ;
    - entre 5 et 8 points : le risque est évalué au niveau 2 (risques modérés) ;
    - plus de 8 points : le risque est évalué au niveau 3 (risques significatifs).

21. En cas de doute entre deux niveaux, la CNIL recommande de retenir le plus élevé. Il appartient à l'organisateur du scrutin, maitrisant le périmètre, les enjeux et le contexte de celui-ci, de retenir le niveau de risque qu'il juge approprié, sachant qu'il pourra être amené à justifier son analyse.

22. La détermination du niveau de risque par l'organisateur du scrutin pouvant être évaluée par l'expert indépendant mandaté pour garantir la conformité des opérations de vote à la présente recommandation (voir ci-après), il convient que l' organisateur du scrutin lui fournisse, le cas échéant, les éléments ayant été pris en compte à cette fin.

23. Par ailleurs, la CNIL recommande au responsable de l'opération de vote de réaliser une analyse d'impact relative à la protection des données (AIPD). Dans le cas d'un scrutin de niveau 3, la réalisation d'une AIPD est susceptible de constituer une obligation au regard des risques pour les personnes concernées, en particulier si le traitement implique la collecte de données sensibles (opinions politiques, appartenances syndicales) à large échelle.

5. Objectifs de sécurité à atteindre en fonction du niveau de risque

24. Chaque niveau de risque identifié par la CNIL se voit associer des objectifs de sécurité qui permettent de définir le niveau de sécurité minimum attendu pour le scrutin. Ces objectifs sont cumulables. Ainsi, les niveaux 2 et 3 ajoutent de nouveaux objectifs complétant les objectifs du ou des niveaux précédents.

25. La présente recommandation peut être lue en correspondance avec le guide de sécurité de l'ANSSI relatif à la sécurité du vote par correspondance électronique, qui propose pour chacun de ces objectifs des explications plus détaillées, ainsi que des solutions adaptées au cas général ainsi qu'à certains contextes particuliers.

26. La CNIL recommande que les solutions de vote dont le scrutin présente un risque de niveau 1 atteignent *a minima* l'ensemble des objectifs de sécurité suivants :

    - Objectif de sécurité n° 1-01 : Mettre en œuvre une solution technique et organisationnelle ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers) et respectant les recommandations de déploiement et d'utilisation émanant de l'éditeur du système de vote électronique retenu et de l'ANSSI.
    - Objectif de sécurité n° 1-02 : Définir le vote d'un électeur comme une opération comportant de manière indivisible la validation de son suffrage, 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. Si une procédure de recouvrement des accès à la plateforme de vote est mise en place, s'assurer que celle-ci n'abaisse pas le niveau de sécurité de l'authentification des électeurs[2].
- Objectif de sécurité n° 1-04 : Assurer la stricte confidentialité de l'expression du vote dès la création du bulletin 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 l'électeur et l'expression de son vote (le contenu déchiffré de son bulletin de vote) pendant toute la durée du traitement, y compris lors du dépouillement et, le cas échéant, lors de l'archivage des données du scrutin.
- Objectif de sécurité n° 1-08 : Renforcer la confidentialité des bulletins de vote en répartissant le secret permettant leur dépouillement, notamment 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 : Assurer que le dépouillement d'une urne n'est réalisable que sur l'ensemble des bulletins qu'elle contient et après la fermeture du scrutin.
- Objectif de sécurité n° 1-10 : Assurer l'intégrité du système de vote électronique et la vacuité de l'urne et de la liste d'émargement avant l'ouverture du scrutin.
- Objectif de sécurité n° 1-11 : Assurer que le bon dépouillement de l'urne peut être vérifié a posteriori.

27. La CNIL recommande que les solutions de vote dont le scrutin présente un risque de niveau 2 atteignent *a minima* l'ensemble des objectifs de sécurité du niveau 1 ainsi que les suivants :

- Objectif de sécurité n° 2-01 : Assurer, durant la période d'ouverture du scrutin, une haute disponibilité du système de vote électronique et des services tiers pouvant être nécessaires à son fonctionnement (notamment pour l'authentification et l'émargement des électeurs, le contrôle par le bureau de vote, etc.).
- Objectif de sécurité n° 2-02 : Mettre en œuvre, sous la surveillance du bureau électoral, un contrôle automatique de l'intégrité du système de vote et de la cohérence entre le contenu de l'urne et le nombre d'émargements pendant toute la durée du scrutin.
- Objectif de sécurité n° 2-03 : Permettre le déclenchement manuel par le bureau électoral des contrôles mentionnés dans l'objectif 2-02. Prévoir la formation du bureau électoral au fonctionnement des outils de contrôle dont il dispose.
- Objectif de sécurité n° 2-04 : Assurer que le bureau électoral soit alerté automatiquement et immédiatement de tout incident de sécurité et de toute intervention de gestion ou de maintenance survenant sur le système de vote électronique et dispose d'un accès à un journal de ces alertes.

[2] Voir notamment les points 17 à 19 de la décision du conseil d'État N° 437993 du 26 janvier 2021 (8ème - 3ème chambres réunies).

- Objectif de sécurité n° 2-05 : Assurer un cloisonnement entre les systèmes de vote électronique de chaque scrutin de sorte qu'aucune donnée ne puisse être échangée entre ces systèmes et qu'il soit possible de suspendre ou 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 des briques applicatives constituant la solution de vote, par la CNIL et par l'ANSSI.
- Objectif de sécurité n° 2-07 : Permettre aux électeurs de vérifier la présence de leur bulletin dans l'urne pendant le scrutin ainsi que sa présence dans l'urne utilisée pour le dépouillement jusqu'à expiration des délais de recours.
- Objectif de sécurité n° 2-08 : Authentifier les électeurs en s'assurant que la vraisemblance d'une usurpation d'identité est négligeable.
- Objectif de sécurité n° 2-09 : Favoriser la transparence et l'auditabilité de la solution de vote en rendant publics, en amont du scrutin, le protocole de vote ainsi que les propriétés de sécurité garanties par ce protocole et le moyen de les atteindre.

28. La CNIL recommande que les solutions de vote dont le scrutin présente un risque de niveau 3 atteignent *a minima* l'ensemble des objectifs de sécurité des niveaux 1 et 2 ainsi que les suivants :
    - Objectif de sécurité n° 3-01 : Effectuer une analyse de risque selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte spécifique du scrutin.
    - Objectif de sécurité n° 3-02 : Assurer que le bon dépouillement de l'urne peut être vérifié a posteriori, y compris par un outil tiers, sans affaiblir le secret du scrutin.
    - Objectif de sécurité n° 3-03 : Assurer, durant la période d'ouverture du scrutin, une très haute disponibilité du système de vote électronique et des services tiers nécessaires à son fonctionnement, en prenant notamment en compte les risques d'avarie majeure comme la perte d'un centre de données.
    - Objectif de sécurité n° 3-04 : Renforcer le caractère secret du scrutin en ne manipulant jamais le secret permettant leur dépouillement sur un serveur qui serait en capacité de rapprocher l'identité des électeurs de leur bulletin.
    - Objectif de sécurité n° 3-05 : Favoriser la transparence de la solution de vote et la confiance des électeurs en rendant public, en amont du scrutin, le code source des éléments du système de vote ayant vocation à être exécutés sur le terminal de l'électeur, y compris dans un navigateur.
29. Il revient au responsable de traitement ou à son prestataire de déterminer les moyens permettant d'atteindre les objectifs de sécurité énoncés, ces choix devant être documentés.

6. Information des électeurs et accessibilité du vote

30. Quel que soit le niveau de risque du scrutin, la CNIL recommande de fournir aux électeurs, en temps utile et en amont de l'élection, une note explicative et facilement compréhensible détaillant les opérations de vote et les différentes étapes leur permettant de voter, ainsi que le

fonctionnement général du système de vote par correspondance électronique. Cette notice explicative ne se substitue pas aux obligations de transparence et d'information imposées par les articles 12, 13 et 14 du RGPD s'agissant du traitement de données à caractère personnel. Ces différentes informations devraient être facilement accessibles à partir de tous les supports de communication ou plateformes en ligne à destination des électeurs.

31. La CNIL recommande que les électeurs soient informés, de manière claire et compréhensible, de la manière dont leur bulletin de vote est pris en compte et traité par le système de vote par correspondance électronique. Cette information porte également, lorsque de tels traitements sont mis en œuvre, sur les traitements statistiques appliqués aux résultats ou les traitements liés à des scrutins indirects. Elle doit permettre aux électeurs de comprendre les principes généraux selon lesquels leur vote contribue au résultat du scrutin, dans le respect du secret du vote et des exigences de sécurité du système.

32. En outre, la CNIL souligne l'importance d'assurer l'accessibilité du vote pour tous les électeurs, qui conditionne la sincérité des opérations électorales. Ainsi, les systèmes de vote par correspondance électronique devraient être accessibles aux personnes en situation de handicap, notamment visuel.

33. En particulier, pour les organismes du secteur public ou délégataires d'une mission de service public désirant proposer ce service aux 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.

34. Enfin, le recours exclusif au vote par correspondance électronique ne devrait pas constituer un obstacle pour les électeurs qui ne disposeraient pas de compétences informatiques ou d'un accès régulier à du matériel et un réseau adaptés. La CNIL recommande aux organisateurs de scrutins de s'assurer de l'accessibilité du vote à ces électeurs, par exemple en mettant à leur disposition un équipement informatique sécurisé et dédié au vote, un accompagnement humain dans le respect du secret et de la liberté du vote, ou, à défaut, des modalités de vote alternatives.

7. Expertise de la solution de vote par correspondance électronique

35. Avant son premier déploiement par un responsable de traitement, la CNIL recommande qu'une expertise indépendante soit réalisée sur toute solution de vote par correspondance électronique, aussi bien pour les SVE développées par les organisateurs de scrutins eux-mêmes, que pour celles fournies par un tiers. Cette première expertise peut, le cas échéant et sous réserve de garantir l'indépendance de l'expert, être commanditée par le fournisseur de la solution.

36. En raison de la complexité des mécanismes techniques mis en œuvre, du caractère sensible des données traitées et du fait que certaines atteintes peuvent demeurer indétectables pour les électeurs, la CNIL recommande par ailleurs que des expertises indépendantes soient régulièrement mises en œuvre en conditions opérationnelles par les organisateurs de scrutins lors du déploiement de systèmes de vote par correspondance électronique.

37. L'expertise indépendante vise à vérifier, de manière objective et approfondie, que le système et, le cas échéant, son environnement de déploiement, garantissent le secret du vote, l'intégrité des suffrages, la sincérité des opérations électorales et la possibilité d'un contrôle a posteriori, notamment en cas de contestation du scrutin. L'ensemble des opérations et vérifications effectuées dans ce cadre devraient être précisées dans un rapport d'expertise.

38. L'expertise d'un système de vote par correspondance électronique devrait être réalisée par un ou plusieurs experts indépendants répondant aux critères suivants :

    - être un informaticien spécialisé dans la sécurité ;
    - ne pas présenter de conflit d'intérêt avec l'entité organisatrice du scrutin qui a décidé d'utiliser la solution de vote, ni avec le fournisseur, le cas échéant, du système de vote à expertiser ou d'autres éléments du système d'information permettant la mise en œuvre du vote par correspondance électronique ;
    - posséder une expérience dans l'analyse des systèmes de vote, si possible, en ayant expertisé les systèmes de vote par correspondance électronique d'au moins deux prestataires différents.

39. Pour leur travail d'évaluation, la CNIL invite les experts à s'appuyer également sur la version la plus récente du guide de sécurité publié par l'ANSSI relatif à la sécurité des systèmes de vote par correspondance électronique.

40. Pour les scrutins présentant un niveau de risque significatif (niveau 3), la CNIL recommande qu'une expertise indépendante soit réalisée à l'occasion de chaque élection. Cette expertise devrait permettre d'évaluer l'effectivité des mesures répondant aux objectifs de sécurité précédemment définis et porter sur l'intégralité de la solution de vote et des éléments décrits dans la présente recommandation, à savoir :

    - La solution de vote en tant que logiciel, incluant :
        - le code source correspondant à la version du système de vote effectivement mise en œuvre pour le scrutin ;
        - les mécanismes cryptographiques utilisés, notamment pour mettre en œuvre les principes fondamentaux qui commandent les opérations électorales ;
        - les mécanismes de scellement utilisés aux différentes étapes du scrutin ;
        - la cohérence entre les éléments publiés relatifs au système de vote, notamment le protocole de vote, et la solution de vote effectivement déployée.
    - Les conditions de mise en œuvre et d'exploitation de la solution de vote, incluant :
        - les systèmes informatiques sur lesquels ont lieu les différentes étapes des opérations électorales, y compris durant le scrutin et après sa clôture (dépouillement, archivage, etc.) ;
        - les modalités d'administration du système de vote ;
        - la gestion des secrets de l'élection ;
    - Les modalités spécifiques au scrutin, incluant :
        - l'évaluation du niveau de risque du scrutin ;
        - la constitution des listes électorales et l'enrôlement des électeurs dans le système ;

- les mécanismes d'authentification des électeurs et les modalités de transmission de leurs moyens d'authentification ;
- la pertinence de la documentation accompagnant le système de vote et de la notice explicative fournie aux électeurs ;
- l'accessibilité du système de vote et la prise en compte des électeurs ne disposant pas de compétences informatiques ou de matériel adaptés.

41. La CNIL recommande également que l'expert vérifie 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.

42. Pour les scrutins présentant un niveau de risque inférieur (niveau 1 ou 2), l'organisateur du scrutin peut décider de l'opportunité de réaliser une expertise pour le scrutin concerné, sans préjudice d'application, le cas échéant, de la réglementation à laquelle il est soumis.

43. Lorsque l'organisateur du scrutin recourt à une expertise pour un scrutin présentant un niveau de risque de niveau 1 ou 2, la CNIL considère qu'il peut définir le périmètre de l'expertise indépendante à partir des éléments détaillés ci-dessus pour les scrutins de risque significatif, en les adaptant à son contexte de mise en œuvre, notamment réglementaire. L'expert peut, selon les besoins exprimés, intervenir pour assister l'organisateur du scrutin dans la rédaction de son cahier des charges, pour auditer une solution afin de vérifier qu'elle couvre les exigences de sécurité attendues, ou encore pour accompagner le déploiement et l'utilisation opérationnelle de la solution lors du scrutin.

44. Pour de tels scrutins, la CNIL considère que des éléments issus d'un rapport d'expertise antérieur et portant sur les briques logicielles de la solution de vote peuvent être repris, dès lors que l'expertise effectuée sur l'élément en question n'est pas antérieure à 24 mois pour un scrutin de niveau 1 ou à 12 mois pour un scrutin de niveau 2, qu'il est possible de vérifier que l'élément sur lequel a porté l'expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.

45. Dans tous les cas, le rapport d'expertise est remis à l'organisateur du scrutin ainsi qu'aux éventuels prestataires impliqués dans le développement et la mise en œuvre de la solution de vote par correspondance électronique.

46. L'expert pouvant avoir 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 utiles afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source non-publié au sein de son 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.

8. Déroulement du vote

47. La CNIL recommande que les heures d'ouverture et de fermeture du scrutin électronique puissent être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

48. 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 devraient être utilisés qu'aux fins précitées et ne peuvent être divulgués sous peine de sanctions.

49. La confidentialité des données est également opposable aux techniciens en charge de la gestion ou de la maintenance des systèmes informatiques.

50. Pour se connecter au système de vote, la CNIL recommande que chaque électeur s'authentifie à l'aide d'un moyen correspondant au niveau de risque identifié pour le scrutin, conformément à la présente recommandation et au guide de l'ANSSI sur la sécurité des systèmes de vote par correspondance électronique. Au cours de cette procédure, le serveur de vote vérifie la validité du moyen d'authentification de l'électeur et que celui-ci est bien autorisé à voter.

51. Quand un électeur sélectionne une liste, un candidat ou un vote blanc, ce choix devrait être distingué de manière manifeste à son écran, indépendamment de toute autre information. L'électeur devrait avoir la possibilité de modifier son choix avant de le valider. En principe, la validation de son choix par l'électeur déclenche la formation et l'envoi du bulletin de vote dématérialisé vers le serveur en charge de l'urne électronique. L'électeur reçoit alors la confirmation de son vote et dispose de la possibilité de conserver une trace de cette confirmation. La solution de vote par correspondance électronique devrait par ailleurs proposer toutes les options prévues par les textes applicables, le cas échéant le vote blanc.

52. Dans le cas où plusieurs modalités de vote sont disponibles pour un même scrutin, par exemple lorsque le vote par correspondance électronique est associé au vote à l'urne ou au vote par correspondance postale, il convient que le vote électronique offre aux électeurs les mêmes possibilités de choix que celles exprimables via les autres modalités de vote, afin de ne pas créer de distorsion en fonction du moyen utilisé. Dans le cas où différentes possibilités sont offertes à l'électeur, la CNIL recommande que le responsable du traitement s'assure qu'un électeur ne puisse pas voter deux fois.

9. Garanties pour un contrôle a posteriori

53. Pour des besoins d'audit externe postérieurs au scrutin, notamment en cas de contentieux électoral et sans préjudice des recommandations précédentes, le système de vote par correspondance électronique doit pouvoir fournir les éléments techniques permettant au minimum de prouver 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 s'est déroulé de façon correcte.

10. Conservation des données portant sur l'opération électorale

54. Les fichiers nécessaires à la réalisation d'un contrôle *a posteriori* des opérations électorales (copies des codes sources et exécutables des programmes et du système sous-jacent, matériels de vote, fichiers d'émargement, de résultats, sauvegardes, etc.) 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 l'organisateur du scrutin dans des conditions garantissant le secret du vote.

55. En particulier, s'il existe des preuves mathématiques permettant de vérifier l'exactitude du décompte des suffrages sans procéder à un nouveau dépouillement, la CNIL recommande la suppression des moyens permettant le déchiffrement des bulletins à l'issue du dépouillement, ou, à défaut, leur conservation sécurisée de ces moyens auprès d'un tiers de confiance, c'est-à-dire d'un organisme indépendant des parties impliquées dans le scrutin et offrant des garanties d'impartialité et de sécurité.

56. L'organisateur du scrutin doit prévoir l'obligation, pour ses prestataires de service, de transférer l'ensemble des supports à la personne ou au tiers nommément désigné pour assurer leur conservation. 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 l'organisateur du scrutin et, le cas échéant, des parties concernées ayant manifesté leur volonté d'assister à cette destruction.