Vote par correspondance électronique : la CNIL met à jour sa recommandation

24.4.2026 - | Commission Nationale de l'Informatique et des Libertés

À l'issue d'une consultation publique, la CNIL actualise sa recommandation sur la sécurité des systèmes de vote par correspondance électronique. Elle offre un cadre plus clair et plus opérationnel, en maintenant un haut niveau d'exigence en matière de sécurité, de confidentialité et de sincérité du scrutin.

La recommandation sur la sécurité des systèmes de vote par correspondance électronique s'adresse :

- aux organismes publics et privés qui souhaitent mettre en place de tels systèmes de vote ;
- aux professionnels du secteur, comme les fournisseurs de systèmes de vote et les experts en sécurité informatique.

Elle définit, selon les meilleures pratiques actuelles, les **objectifs de sécurité** que devrait atteindre tout dispositif utilisé lors de votes à bulletin secrets. Elle peut aussi servir de référence, lorsque cela est pertinent, pour la mise en œuvre de scrutins non secrets.

Dans la continuité de la version de 2019, la recommandation repose sur les principes fondamentaux du droit électoral et adapte le niveau de sécurité en fonction des risques liés au scrutin. Elle a pour objectif d'offrir aux responsables de traitement, à leurs prestataires et aux experts un cadre plus clair et actualisé pour l'organisation d'élections.

Pourquoi la CNIL fait-elle évoluer sa recommandation ?

Depuis 2019, le recours au vote par correspondance électronique a continué de se développer et de se diversifier. Ces dispositifs sont aujourd'hui utilisés dans des contextes variés, dans le secteur privé comme dans la fonction publique. Dans le même temps, l'environnement technique et juridique a également évolué, notamment avec les règles désormais applicables à l'organisation des élections des représentants du personnel dans la fonction publique.

Dans ce contexte, il était nécessaire de mettre à jour la recommandation. Cette révision permet de mieux clarifier les attentes et d'offrir aux acteurs un cadre plus cohérent et plus opérationnel. Elle s'appuie aussi sur le retour d'expérience des acteurs concernés, recueilli par la CNIL à travers ses actions d'accompagnement, sa veille, ainsi que les plaintes et les notifications de violations.

Enfin, la CNIL a travaillé en coopération avec l'ANSSI, qui a également publié un guide consacré à la sécurité des systèmes de vote par correspondance électronique.

La recommandation de la CNIL fixe les objectifs de sécurité qu'elle considère comme les meilleures pratiques, selon les types de scrutin. De son côté, le guide de l'ANSSI apporte des précisions et des recommandations techniques pour atteindre ces objectifs.

Ces deux documents sont donc faits pour être utilisés ensemble, de manière cohérente et complémentaire.

Lire la recommandation de la CNIL

Lire le guide de l'ANSSI

Une mise à jour construite avec la contribution des acteurs concernés

La recommandation a également été enrichie par les contributions reçues dans le cadre de la consultation publique menée en 2025. Cette concertation a permis de recueillir de nombreuses observations de la part d'acteurs concernés par le recours au vote par correspondance électronique, qu'il s'agisse d'organisateurs de scrutin, de prestataires fournissant des systèmes de vote, d'experts ou d'autres parties prenantes.

Ces contributions ont permis d'améliorer le projet de la CNIL : le texte est plus clair, certaines exigences ont été précisées et mieux adaptées aux contraintes opérationnelles des acteurs et aux conditions concrètes de mise en œuvre.

Ce qui change avec la nouvelle recommandation

Les principaux points à retenir de la recommandation actualisée :

Elle rappelle les **principes fondamentaux qui encadrent les opérations électorales**. Elle rappelle plus explicitement que les exigences de sécurité doivent être évaluées au regard de ces principes, notamment pour garantir le secret du vote, la sincérité du scrutin, la surveillance effective des opérations électorales et la possibilité d'en vérifier le bon déroulement.

Dans la continuité de la recommandation adoptée en 2019, la nouvelle version conserve une **approche fondée sur le niveau de risque du scrutin** (répartis en trois niveaux, le niveau 3 correspondant au risque le plus élevé), tout en faisant évoluer plusieurs aspects importants. Toutefois, les critères qui permettent d'apprécier ce niveau de risque ont été révisés. L'objectif est de mieux prendre en compte la diversité des scrutins concernés, leur contexte d'organisation et les enjeux qui leur sont propres. Le questionnaire d'auto-évaluation, auparavant disponible sur le site de la CNIL, a été revu et intégré directement dans la recommandation.

La partie consacrée aux **objectifs de sécurité a elle aussi été retravaillée**. Certains objectifs ont été ajoutés, d'autres reformulés, précisés ou réorganisés, afin de rendre le cadre plus lisible et plus cohérent. C'est le cas, par exemple, des objectifs 3.02 (vérifiabilité du bon dépouillement de l'urne) et 3.04 (les modalités de manipulation du secret permettant le dépouillement). À la suite des retours de la consultation publique, plusieurs objectifs ont aussi été reformulés de façon plus neutre sur le plan technologique : la recommandation insiste davantage sur les objectifs à atteindre, tout en laissant aux acteurs le choix des moyens, à condition qu'ils puissent justifier et documenter ces choix.

La recommandation précise aussi les **exigences de transparence**. Elles prévoient notamment la publication en amont du scrutin des spécifications techniques du protocole de vote (objectif de niveau 2) ainsi que la publication du code source du client de vote pour les scrutins les plus sensibles (objectif de niveau 3). L'exigence de transparence s'étend à l'information des électeurs : ils doivent recevoir en amont une note expliquant comment leurs données sont traitées.

Enfin, la recommandation fait **évoluer le cadre de l'expertise indépendante des systèmes de**

vote. Elle met tout d'abord l'accent sur la nécessité, pour tout système de vote, de faire l'objet d'une expertise avant sa première utilisation. Mais les règles varient selon le niveau de risque du scrutin. Pour les scrutins les plus sensibles (niveau 3), une expertise reste attendue pour chaque scrutin. Pour les autres, l'organisateur dispose d'une plus grande latitude et peut, selon les cas, s'appuyer sur une expertise préalable déjà réalisée, sans devoir en refaire une à chaque scrutin. Cette évolution permet de mieux proportionner les exigences aux enjeux du scrutin, tout en maintenant un haut niveau de garantie pour les scrutins les plus sensibles.

Calendrier d'application et ressources utiles

Afin de tenir compte des contraintes des acteurs, la publication de la nouvelle recommandation s'accompagne d'une période de transition. Ainsi, comme la CNIL l'avait indiqué en novembre 2025, les scrutins déjà en préparation et prévus en 2026 pourront continuer à appliquer la version de 2019 de la recommandation.

En revanche, **la nouvelle recommandation s'applique à tout nouveau scrutin.**

https://www.cnil.fr/fr/recommandation-vote-electronique