FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE

GUIDE FNTC · VOTE ÉLECTRONIQUE

Recommandation CNIL 2026 sur le vote électronique : ce qui change et quand

Analyse comparative des délibérations n° 2019-053 et n° 2026-045



Sommaire

— Objet du document 2

1 Les textes et leur place dans la hiérarchie des normes 3

2 Entrée en vigueur : quand appliquer la recommandation 2026 ? 7

3 Un nouveau cadre d’analyse du risque 9

4 Les objectifs de sécurité : comparatif 2019 et 2026 13

5 Les autres évolutions 15

— Références 17

EN BREF

19 mars 2026
Adoption de la délibération n° 2026-045

25 avril 2026
Publication sur Légifrance

3 niveaux
de risque, aux critères et exemples redéfinis

25 objectifs
de sécurité cumulés, contre 23 en 2019

Objet du document

La CNIL a adopté le 19 mars 2026 une nouvelle recommandation relative à la sécurité des systèmes de vote par correspondance électronique (délibération n° 2026-045), qui remplace la recommandation du 25 avril 2019 (délibération n° 2019-053). Le présent document fait le point sur ce nouveau cadre : place des textes dans la hiérarchie des normes, entrée en vigueur, nouvelle méthode d’évaluation du risque, comparaison des objectifs de sécurité 2019 et 2026 et autres évolutions.

1 Les textes et leur place dans la hiérarchie des normes

1.1 Les deux recommandations

	Délibération n° 2019-053	Délibération n° 2026-045
Adoption	25 avril 2019	19 mars 2026
Publication	Légifrance, 22 juin 2019	Légifrance, 25 avril 2026 (NOR : CNIS2610924X)
Nature	Recommandation	Recommandation
Statut	Remplacée par la délibération n° 2026-045	En vigueur ; remplace les délibérations n° 2010-371 et n° 2019-053
Disposition transitoire	Prise en compte par les responsables de traitement après un délai de douze mois à compter de la publication	Aucune dans le texte publié ; tolérance annoncée par la CNIL pour les scrutins prévus en 2026 (partie 2)
Texte d'accompagnement	Fiche pratique annoncée par la CNIL (exemples de moyens)	Guide ANSSI-PA-118 du 24 avril 2026, auquel renvoie la recommandation (CNIL 2026, § 25 et 39)



1.2 Une hiérarchie des textes à plusieurs niveaux



Le guide ANSSI-PA-118 NON NORMATIF

Détaille, objectif par objectif, des moyens de mise en œuvre. Ses recommandations n'ont pas de caractère normatif ; les prestataires restent libres des moyens retenus, l'expertise indépendante évaluant leur pertinence.

La recommandation de la CNIL DOCTRINE

Exprime la doctrine de l'autorité de contrôle. Elle n'a pas, par elle-même, la valeur d'un texte réglementaire et réserve l'application de la réglementation propre à chaque scrutin (par exemple pour l'expertise, CNIL 2026, § 42).
Les textes sectoriels l'emportent en cas de contradiction; la recommandation éclaire leur mise en œuvre.

Les textes législatifs et réglementaires S'IMPOSENT

Principes du droit électoral, RGPD et loi n° 78-17 du 6 janvier 1978, et textes sectoriels propres à chaque scrutin, notamment le code général de la fonction publique (art. R. 211-503 à R. 211-584 CGFP) et le code du travail (art. R. 2314-5 et suivants C. trav.).

À RETENIR

En conséquence, **au regard de la hiérarchie des normes, ni la recommandation n° 2026-045 de la CNIL ni le guide de l'ANSSI ne constitue un texte contraignant en lui-même**. Leur objectif est de faciliter la mise en conformité des systèmes de vote électronique aux textes législatifs et réglementaires applicables aux élections concernées.

Pour autant, **la recommandation de la CNIL, voire le guide de l'ANSSI, peuvent devenir obligatoires** :

Par contrat

Lorsqu'un cahier des charges, un protocole préélectoral ou un marché public s'y réfère : il convient alors de vérifier si la référence vise la version en vigueur au jour de la signature ou la version la plus récente.

Dans les administrations

Si le respect de la recommandation de la CNIL est imposé par une circulaire contraignante. *A contrario*, s'il s'agit d'une circulaire interprétative, la recommandation n'acquiert pas *de facto* un caractère obligatoire. Il conviendra donc d'identifier la nature juridique de la circulaire pour apprécier le caractère contraignant ou non de la recommandation.

EN CAS DE CONTENTIEUX

Par ailleurs, en cas de contentieux, les juridictions saisies de litiges relatifs à des élections peuvent être amenées à se prononcer sur le système de vote électronique (SVE) mis en place. Si le SVE respecte la recommandation de la CNIL, la preuve de sa conformité aux exigences législatives et réglementaires relatives à l'organisation des élections concernées sera plus facile à rapporter. À défaut, l'organisateur de l'élection (avec l'aide de son prestataire si cela est prévu contractuellement) devra démontrer comment le SVE répond aux exigences des textes applicables pour le scrutin concerné. La preuve de la conformité du SVE mis en place aux exigences législatives et réglementaires sera alors plus délicate à rapporter.

POUR L'AUDIT DES SOLUTIONS

Dans la même logique, la recommandation de la CNIL et le guide de l'ANSSI servent en pratique de référentiels aux experts chargés de l'audit des solutions de vote électronique. Un prestataire qui s'y conforme favorisera ainsi la reconnaissance de la conformité du SVE aux exigences imposées par les textes pour le scrutin concerné. À défaut, il devra prouver que les mesures qu'il a choisies de mettre en place répondent aux dispositions applicables en matière de vote électronique. Ce qui peut s'avérer compliqué.

EN CAS DE CONTRÔLE DE LA CNIL

Enfin, et à toutes fins utiles, il est précisé qu'en cas de contrôle, la CNIL pourra utiliser sa recommandation comme référentiel pour apprécier la conformité du SVE à la réglementation relative à la protection des données personnelles. Là encore, si le SVE est conforme à ses préconisations « *protection des données personnelles* », alors la CNIL considérera que la réglementation de protection des données personnelles a été respectée. En revanche, si ses préconisations n'ont pas été prises en compte, l'organisateur de l'élection et/ou le fournisseur devront démontrer comment le SVE respecte les exigences de protection des données personnelles imposées par la loi et expliciter l'adéquation des mesures mises en place ; étant précisé que les sanctions de la CNIL sont quant à elles contraignantes.

2 Entrée en vigueur : quand appliquer la recommandation 2026 ?

Aucune disposition transitoire n'est publiée dans le texte officiel : la délibération n° 2026-045, publiée le 25 avril 2026, remplace la recommandation 2019 sans délai, alors que celle-ci laissait douze mois aux responsables de traitement (CNIL 2019, dispositions transitoires et finales).

La CNIL a néanmoins annoncé une **période de transition** dans sa communication du 24 avril 2026 accompagnant la publication, comme elle l'avait indiqué dès novembre 2025 : **les scrutins déjà en préparation et prévus en 2026 peuvent continuer à appliquer la recommandation 2019** ; la recommandation 2026 s'applique à **tout nouveau scrutin**.

REPÈRES CHRONOLOGIQUES

25 avril 2019	Adoption de la délibération n° 2019-053, avec un délai de douze mois pour sa prise en compte
Novembre 2025	La CNIL indique une future période de transition
19 mars 2026	Adoption de la délibération n° 2026-045
24 avril 2026	Communication de la CNIL annonçant la période de transition · guide ANSSI-PA-118
25 avril 2026	Publication sur Légifrance : la recommandation 2026 remplace celle de 2019, sans délai
Décembre 2026	Élections professionnelles de la fonction publique, dans le champ de la tolérance annoncée
À partir de 2027	La recommandation 2026 s'applique à tout scrutin

Scrutin prévu en 2026 et déjà en préparation

→ **Recommandation 2019 possible**

Tout nouveau scrutin

→ **Recommandation 2026**

Conséquences pratiques à anticiper :

- **Scrutins prévus en 2026 et déjà en préparation** : ils peuvent rester sur la recommandation 2019. L'organisateur a intérêt à conserver la trace de l'engagement de la préparation avant la publication et à identifier, dès à présent, les écarts avec la recommandation 2026.

- **Tout nouveau scrutin** : la recommandation 2026 s'applique.

- **Marchés et contrats en cours** : vérifier la rédaction de la clause de référence (statique ou dynamique) et, le cas échéant, prévoir un avenant ou une mise à niveau.

- **Élections professionnelles de la fonction publique de décembre 2026** : elles relèvent des art. R. 211-503 à R. 211-584 CGFP issus du décret n° 2024-1038 du 6 novembre 2024 ; en préparation et prévues en 2026, elles entrent dans le champ de la tolérance annoncée par la CNIL.

- ! **Objectifs structurants** (par exemple **3-04** et **3-05** pour les scrutins de niveau 3) : ils peuvent nécessiter des évolutions d'architecture ; un plan de mise à niveau des solutions est à établir sans attendre.



3 Un nouveau cadre d’analyse du risque

3.1 Trois niveaux de risque redéfinis

Les trois niveaux sont conservés, mais leurs critères et leurs exemples évoluent (CNIL 2026, § 17) :

Niveau	Recommandation 2019	Recommandation 2026
Niveau 1 Risques faibles	Peu d’électeurs, cadre non conflictuel, élus ayant peu de pouvoirs. Exemple : élection d’un représentant de classe	Mêmes critères, auxquels s’ajoute l’absence de révélation des orientations politiques ou des opinions syndicales. Exemples : représentants de parents d’élèves, associations locales
Niveau 2 Risques modérés	Nombre **important** d’électeurs, enjeu élevé, pas de conflictualité particulière. Exemples : représentants du personnel au sein d’organismes, **ordre professionnel**	Nombre **modéré** de votants, enjeu moyen, pas de conflictualité particulière. Exemple : représentants du personnel au sein d’organismes de petite ou moyenne taille
Niveau 3 Risques significatifs	Nombre important d’électeurs, enjeu très élevé **et** climat potentiellement conflictuel. Exemple : représentants du personnel au sein d’organisations importantes, à grande échelle et dans un cadre conflictuel	Nombre important de votants, enjeu élevé **ou** climat potentiellement conflictuel. Exemples : **ordres professionnels réglementés**, primaires de partis politiques, représentants du personnel au sein d’organisations importantes

CE QUI CHANGE

et → ou

Le niveau 3 n’exige plus la réunion d’un enjeu élevé et d’un climat conflictuel : l’un ou l’autre suffit.

N2 → N3

Les ordres professionnels passent du niveau 2 au niveau 3.

+ menace

Les fournisseurs du système de vote figurent désormais explicitement parmi les sources de menace à tous les niveaux.

La CNIL maintient sa recommandation de ne pas recourir au vote électronique lorsque les sources de menace disposent à la fois de ressources importantes et d'une forte motivation, et cite désormais l'exemple de risques d'ingérence étrangère (CNIL 2026, § 18). Elle se dit « très réservée » pour les scrutins politiques ; pour ceux que la loi ouvre déjà au vote électronique (votes des Français de l'étranger), elle estime qu'il convient d'appliquer a minima les recommandations du niveau de risque le plus élevé (CNIL 2026, § 10).

L'ÉCLAIRAGE DU GROUPE DE TRAVAIL FNTC

10 000
électeurs · élection du CSE

100 000
électeurs · élections au sein de mutuelles

À titre d'exemple, le groupe de travail e-vote de la FnTC considère qu'une élection du CSE avec 10 000 électeurs peut être considérée comme « un nombre important de votants », ce seuil montant à 100 000 électeurs pour des élections au sein de mutuelles.



3.2 Une grille d’analyse intégrée à la recommandation

En 2019, la grille d’analyse était proposée « de manière facultative et à titre d’exemple » dans une fiche pratique distincte (CNIL 2019, niveau de risque du scrutin). En 2026, elle figure dans la recommandation elle-même, avec un barème (CNIL 2026, § 19 et 20). Son usage reste facultatif et le résultat indicatif.

Questions valant 1 point

- **Q1** plus de 250 personnes
- **Q2** plus de 2 000 personnes
- **Q3** attaques informatiques subies par l’organisateur dans les cinq dernières années
- **Q4** contentieux sur des scrutins similaires dans les cinq dernières années
- **Q5** accès de personnes intéressées au résultat aux données de renouvellement d’accès
- **Q6** révélation possible d’opinions politiques, philosophiques ou syndicales
- **Q7** organisateur entité importante ou essentielle au sens de NIS 2
- **Q8** intérêt des données pour un attaquant
- **Q9** statut protecteur des élus
- **Q10** pouvoirs organisationnels ou financiers des élus
- **Q11** première mise en œuvre du vote électronique par l’organisateur

Questions valant 2 points

- **Q12** pouvoirs de sanction des élus à l’égard de tiers
- **Q13** désignation de candidats à une élection politique (primaires)
- **Q14** développements techniques spécifiques importants

BARÈME

0 à 4 points	Niveau 1
5 à 8 points	Niveau 2
Plus de 8 points	Niveau 3

Barème : **0 à 4 points : niveau 1 ; 5 à 8 points : niveau 2 ; plus de 8 points : niveau 3**. En cas de doute, le niveau le plus élevé est retenu ; l’organisateur peut retenir le niveau qu’il juge approprié, à charge de justifier son analyse, que l’expert indépendant peut évaluer (CNIL 2026, § 21 et 22).

3.3 Une analyse du risque élargie

L’analyse porte aussi sur le respect des obligations liées aux données personnelles des électeurs, et pas seulement sur les principes du droit électoral : un accès non autorisé au fichier des électeurs peut constituer une violation de données sans affecter la sincérité du scrutin (CNIL 2026, § 13 et 14).

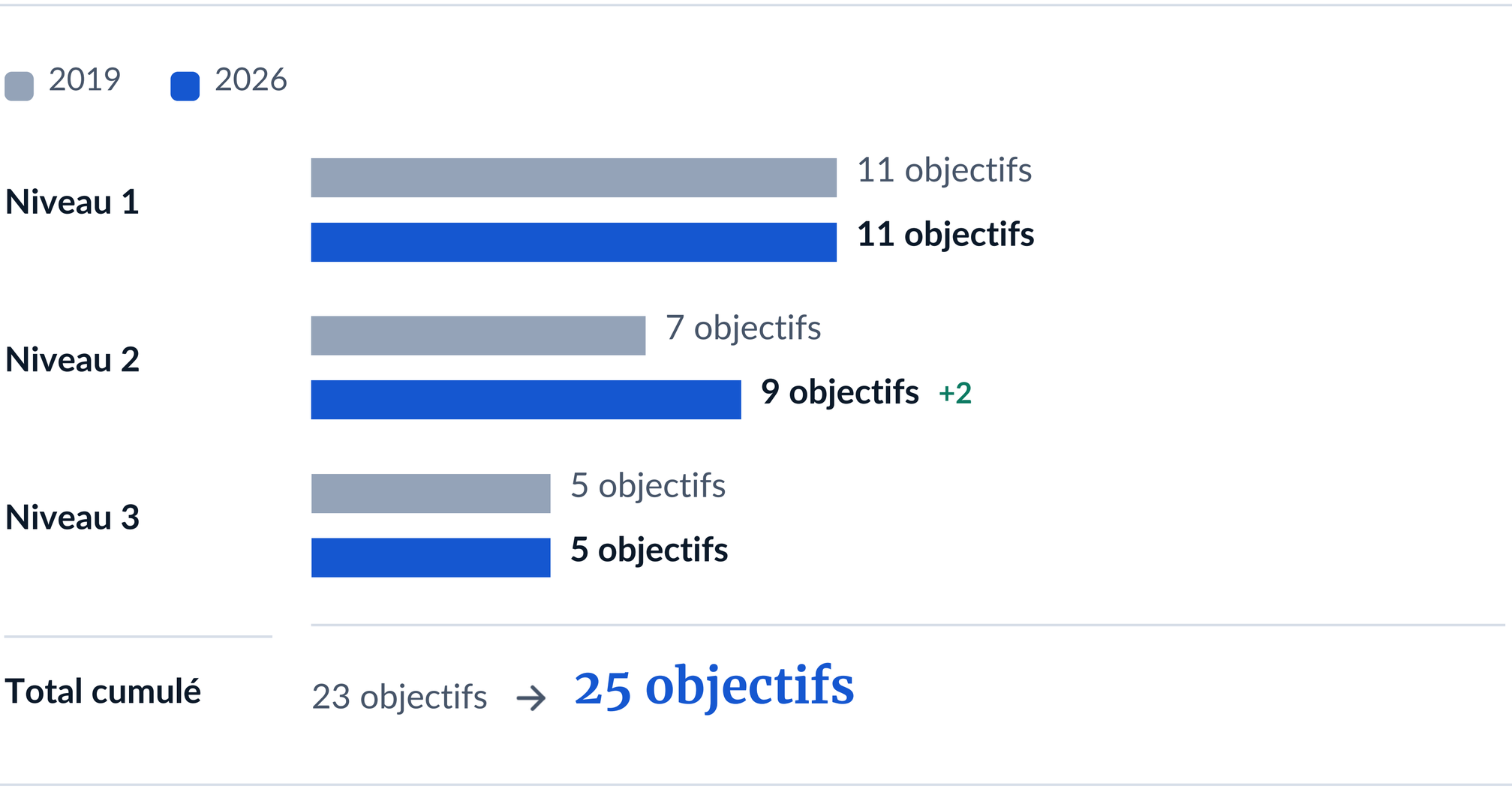
Les facteurs humains et organisationnels sont à prendre en compte : temps et moyens disponibles, expérience des équipes, compétences numériques des électeurs (CNIL 2026, § 15).

L’analyse d’impact relative à la protection des données (AIPD) est recommandée dans tous les cas, et susceptible de constituer une obligation pour un scrutin de niveau 3 (CNIL 2026, § 23). En 2019, la CNIL indiquait seulement qu’une AIPD pouvait être nécessaire (CNIL 2019, niveau de risque du scrutin).



4 Les objectifs de sécurité : comparatif 2019 et 2026

4.1 Vue d’ensemble



Les objectifs restent cumulatifs. La numérotation est en partie conservée, mais plusieurs objectifs changent de contenu à numéro identique (notamment **2-04**, **3-04** et **3-05**) : la comparaison doit se faire sur le fond, et non sur le seul numéro. Il revient au responsable de traitement ou à son prestataire de déterminer les moyens pour atteindre les objectifs, ces choix devant désormais être **documentés** (CNIL 2026, § 29).



4.2 Les exigences nouvelles ou renforcées à retenir

Transparence et vérifiabilité

Publication du protocole de vote (**CNIL 2026 : 2-09**) et du code source client (**CNIL 2026 : 3-05**), vérifiabilité individuelle dans la durée (**CNIL 2026 : 2-07**) et vérifiabilité universelle par un outil tiers (**CNIL 2026 : 3-02**).

Supervision par le bureau électoral

Dès le niveau 2 : contrôles automatiques et déclenchement manuel (**CNIL 2026 : 2-02, 2-03**), alertes immédiates et journal des incidents et interventions (**CNIL 2026 : 2-04**), formation du bureau.

Protection du secret

Séparation entre le secret de dépouillement et tout serveur capable de rapprocher identité et bulletin (**CNIL 2026 : 3-04**), étanchéité étendue au dépouillement et à l'archivage (**CNIL 2026 : 1-07**).

Authentification

Vraisemblance d'usurpation négligeable au niveau 2 (**CNIL 2026 : 2-08**) et sécurisation des procédures de recouvrement des accès dès le niveau 1 (**CNIL 2026 : 1-03**).

Disponibilité et cloisonnement

Services tiers intégrés (**CNIL 2026 : 2-01, 3-03**), perte d'un centre de données au niveau 3, cloisonnement sans échange de données entre scrutins (**CNIL 2026 : 2-05**).

4.3 Ce qui disparaît ou change de place

3-05 → 2-05 2019 → 2026	Le **cloisonnement physique** entre prestations de vote (3-05, CNIL 2019) n'est plus exigé en tant que tel ; il est remplacé par un cloisonnement sans échange de données, dès le niveau 2 (CNIL 2026 : 2-05).
3-04 → 2-03 2019 → 2026	Le **contrôle manuel** de l'intégrité par le bureau (3-04, CNIL 2019) descend au niveau 2 (CNIL 2026 : 2-03).
2-04 → 2-08 2019 → 2026	L'**authentification renforcée** du niveau 2 change de numéro (2-04 CNIL 2019, devenu 2-08 CNIL 2026).

5 Les autres évolutions

Principes fondamentaux

Aux principes rappelés en 2019 (secret, caractère personnel et libre du vote, sincérité, surveillance effective, contrôle a posteriori) s'ajoutent l'intégrité des suffrages exprimés et l'accès au vote pour tous les électeurs (CNIL 2026, § 8).

Information des électeurs

La notice explicative doit être facilement compréhensible et accessible depuis tous les supports ; les électeurs sont informés de la manière dont leur bulletin est pris en compte, y compris lors de traitements statistiques ou de scrutins indirects (CNIL 2026, § 30 et 31).

Accessibilité

Le respect du Référentiel général d'amélioration de l'accessibilité (RGAA) reste exigé pour le secteur public ; le recours exclusif au vote électronique ne doit pas exclure les électeurs sans compétences ou matériel adaptés (équipement dédié, accompagnement humain ou modalité alternative) (CNIL 2026, § 32 à 34).

Expertise indépendante

EN 2019

Tout responsable de traitement devait faire expertiser sa solution, avec réutilisation possible d'éléments antérieurs aux niveaux 1 et 2 (CNIL 2019, expertise du système de vote).

EN 2026

Expertise avant le premier déploiement (CNIL 2026, § 35), expertise à chaque élection pour le niveau 3 (CNIL 2026, § 40), opportunité laissée à l'organisateur pour les niveaux 1 et 2, sans préjudice de la réglementation applicable (CNIL 2026, § 42), réutilisation dans les mêmes limites de 24 et 12 mois pour l'analyse logicielle (CNIL 2026, § 44).

Le rapport est remis à l'organisateur et aux prestataires (CNIL 2026, § 45). Les textes sectoriels restent applicables : dans la fonction publique, l'expertise accompagne chaque scrutin (art. R. 211-518 et R. 211-519 CGFP) ; pour le CSE, elle est requise à la mise en place du système et à chaque modification substantielle (art. R. 2314-9 C. trav. ; Cass. soc., 26 mars 2025, n° 24-12.607).

Conservation des données

Conservation sous scellés sous le contrôle de l’organisateur du scrutin (et non plus de la commission électorale, CNIL 2019) ; lorsque des preuves mathématiques permettent de vérifier le décompte sans nouveau dépouillement, la CNIL recommande de supprimer les moyens de déchiffrement après le dépouillement ou de les confier à un tiers de confiance ; la destruction peut se faire en présence des parties qui l’ont demandée (CNIL 2026, § 54 à 56).



Références

1. CNIL, 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 (remplacée).

2. CNIL, délibération n° 2026-045 du 19 mars 2026 portant adoption d’une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, publiée le 25 avril 2026.

3. CNIL, « Vote par correspondance électronique : la CNIL met à jour sa recommandation », communication du 24 avril 2026 (calendrier d’application et période de transition), cnil.fr.

4. ANSSI, guide ANSSI-PA-118 « Recommandations pour la mise en œuvre du vote par Internet pour les élections non politiques », v1.0 du 24 avril 2026.

5. Code général de la fonction publique, art. R. 211-503 à R. 211-584 (décret n° 2024-1038 du 6 novembre 2024) ; code du travail, art. R. 2314-5 et suivants.

Comité de rédaction :

- **Cabinet Caprioli & Associés**
- **Euro-vote**
- **LegaVote**
- **LEHM Expertises**
- **Slib**
- **VCAST**
- **Voxaly**

La Fédération des Tiers de Confiance du numérique (FnTC) rassemble éditeurs de logiciels, prestataires de services, experts, professionnels réglementés, start up, acteurs internationaux, utilisateurs et structures institutionnelles.

Notre objectif depuis 2001 : **une digitalisation fiable et sécurisée.**

Notre méthode :

- Produire des expertises et des outils pour que les personnes et les organisations puissent au sein du monde numérique préserver leurs droits et limiter leurs risques.
- Elaborer de la doctrine, en produisant des guides, des référentiels et des labels.
- Participer à la normalisation et à la standardisation des bonnes pratiques numériques au niveau national (Afnor) et international (ISO)
- Assurer des formations universitaires, comme les Masters Droit du numérique des Universités de Corse, de La Rochelle et de Lyon.

Fédération des Tiers de Confiance du numérique
Groupe de travail vote électronique
5 impasse Gomboust, 75001 Paris
fntc-numerique.com

Novembre 2026