Expertise indépendante du système de vote mis en œuvre pour les élections des représentants au Conseil d'administration au Conseil académique, au Conseil de pôle humanités, au Conseil de pôle sociétés, au Conseil de pôle santé et au Conseil de pôle sciences et technologie de l'Université de Nantes

Rapport d'expertise préliminaire

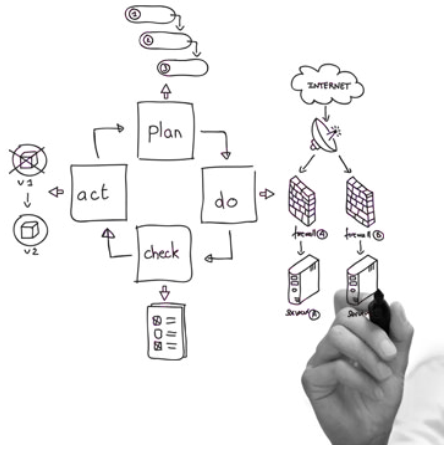

Table des matières

Auteur :	Sébastien Roman	ITekia	sebastien.roman@itekia.com
Date	18/11/2021	Version	01
Référence	ITekia / UNIVNANTES / 2021 / 11 / 18 / INI / 01		
Version	Date	Objet de la modification	
01	18/11/2021	Version initiale	

1 Introduction

1.1 Élections des représentants des personnels et des usagers et rôle de l'expert

Le décret n°2020-1205 du 30 septembre 2020 relatif à l'élection ou la désignation des membres du Conseil national de l'enseignement supérieur et de la recherche et des conseils des établissements publics d'enseignement supérieur relevant du ministre chargé de l'enseignement supérieur, autorise l'utilisation du vote électronique dans les conditions fixées par les articles n°2 à 17 décret n°2011-595[1].

Le décret n°2011-595 du 26 mai 2011 ouvre la possibilité de recours au vote électronique pour les élections des représentants du personnel au sein des instances de représentation du personnel de la fonction publique de l'État.

L'article 7 de ce même décret impose la réalisation d'une expertise indépendante du système de vote électronique. Selon cet article, cette expertise est destinée à vérifier le respect des garanties prévues dans ce même décret, qui rappelle dans l'alinéa 2 de l'article 2 les contraintes générales que doivent respecter les systèmes de vote électronique mis en œuvre dans le cadre de ces élections, à savoir :

« Le recours au vote électronique par internet est organisé dans le respect des principes fondamentaux qui commandent les opérations électorales, notamment la sincérité des opérations électorales, l'accès au vote de tous les électeurs, le secret du scrutin, le caractère personnel, libre et anonyme du vote, l'intégrité des suffrages exprimés, la surveillance effective du scrutin et le contrôle a posteriori par le juge de l'élection. »

Ce décret précise différentes modalités organisationnelles du vote électronique. Notons néanmoins qu'il ne précise pas les modalités techniques que le système de vote doit mettre en œuvre afin de respecter les principes fondamentaux du droit électoral énoncés dans l'alinéa 2 de l'article 2, ce qui pourrait ouvrir la voie à un débat d'expert sur ces mêmes modalités techniques.

Toutefois, la CNIL a régulièrement publié des délibérations portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique notamment via Internet. A travers ses recommandations, la CNIL « *souligne que le recours à de tels systèmes doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin sauf pour les scrutins publics, le caractère personnel et libre du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l'élection. »*

L'objectif de ces recommandations est de *« fixer, de façon pragmatique, les objectifs de sécurité que doit atteindre tout dispositif de vote par correspondance électronique, notamment via Internet, en fonction des risques que présente le déroulement du vote. »*[2]

Comme le rappelle le paragraphe 4 de la décision du conseil d'état n°368748 du 11 mars 2015, la CNIL peut procéder par voie de recommandation pour l'accomplissement de ses missions.

1 L'article 7 du décret n°2020-1205 indique *« – I. – A titre expérimental, l'élection des représentants des personnels et des étudiants aux conseils des établissements publics à caractère scientifique, culturel et professionnel et des établissements publics nationaux d'enseignement supérieur à caractère administratif peut avoir lieu par vote électronique. A l'exception du III de l'article 2, du 7 o de l'article 5 et de l'article 15 du décret du 26 mai 2011 précité, ce recours au vote électronique est organisé dans les conditions fixées par les articles 2 à 17 de ce même décret.*
II. – Pour l'application de l'article 5 du décret du 26 mai 2011 précité, les modalités d'organisation du vote électronique sont fixées :
1 S'agissant des modalités prévues aux 1 o , 4 o et 5 o de cet article, par décision de l'autorité administrative habilitée en charge de l'organisation des élections, après avis du comité électoral consultatif avant chaque élection ;
2 S'agissant des modalités prévues aux 2 o , 3 o et 6 o de cet article, par arrêté de l'autorité administrative habilitée en charge de l'organisation des élections, pris après consultation du comité technique compétent et du comité électoral consultatif. »

2 Délibération CNIL 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

Ce même article rappelle également que la CNIL est à bon droit d'interpréter les dispositions législatives et réglementaires applicables en matière de vote électronique et à recommander la mise en place de mesures visant à garantir le respect de ces dispositions.

Les délibérations successives de la CNIL constituent donc, de notre point de vue, l'interprétation de référence de ces mêmes dispositions législatives et réglementaires, en particulier sur les mesures de sécurité techniques à mettre en œuvre lors du recours au vote par voie électronique. A ce titre, elles doivent clore nombre de débats d'experts sur le choix des mesures techniques à mettre en place.

A noter que la délibération de la CNIL actuellement en vigueur est relativement récente. Il s'agit de la délibération n°2019-053 du 15 avril 2019. Elle est parue au journal officiel le 21 juin 2019 pour être prise en compte par les organisateurs du scrutin à partir du 21 juin 2020.

Ni la délibération CNIL n°2019-053 ni le décret n°2011-595 ne demandent à ce que l'expert se prononce sur l'opportunité de réaliser les élections avec le système expertisé dans les conditions telles que décrites à l'expert. **Nous n'émettrons donc pas d'avis dans un sens ou dans un autre.**

Le choix de réaliser les élections par voie électronique et le choix du système de vote restent pleinement de la responsabilité des organisateurs des scrutins.

1.2 Périmètre des travaux d'expertise

Le décret n°2011-595 précise que l'expertise indépendante *« couvre l'intégralité du dispositif installé avant le scrutin, les conditions d'utilisation du système de vote durant le scrutin, les conditions d'utilisation du poste dédié mentionné au II de l'article 9 ainsi que les étapes postérieures au vote. »*

En dehors de la mise en place de postes réservés qui est une spécificité du recours au vote électronique dans la fonction publique, la CNIL reprend ces éléments dans sa délibération n°2019-053 : *« l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes d'électeurs et leur enrôlement et l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.). »*

Ces éléments sont ensuite détaillés dans la même délibération :

« L'expertise doit porter sur l'ensemble des éléments décrits dans la présente délibération et notamment sur :

– le code source correspondant à la version du logiciel effectivement mise en œuvre ;

– les mécanismes de scellement utilisés aux différentes étapes du scrutin ;

– le système informatique sur lequel le vote va se dérouler ;

– les échanges réseau ;

– les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote ;

– les mécanismes d'authentification des électeurs et la transmission des secrets à ces derniers ;

– l'évaluation du niveau de risque du scrutin ;

– la pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité.

Cette recommandation CNIL n°2019-053 introduit des niveaux de risques. Chaque niveau de risque se voit associer des objectifs de sécurité qui permettent de définir le niveau de sécurité attendu.

Ces objectifs sont cumulables, le niveau 2 étant composé d'objectifs de sécurité spécifiques et des objectifs de sécurité du niveau 1, le niveau 3 étant, quant à lui, composé d'objectifs de sécurité spécifiques et des objectifs de sécurité des deux niveaux précédents.

S'il appartient à l'organisateur des élections d'identifier le niveau correspondant à sa situation en fonction des risques soulevés par son scrutin, ce choix doit être évalué par l'expert indépendant comme indiqué dans la délibération CNIL.

1.3 Qualités de l'expert indépendant

Si le décret n°2011-595 ne précise pas les qualités de l'expert, la délibération CNIL indique que :

« L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

– être un informaticien spécialisé dans la sécurité ;

– ne pas avoir d'intérêt dans la société qui a créé la solution de vote à expertiser, ni dans l'organisme responsable de traitement qui a décidé d'utiliser la solution de vote ;

– posséder si possible une expérience dans l'analyse des systèmes de vote, en ayant expertisé les systèmes de vote par correspondance électronique, notamment via Internet, d'au moins deux prestataires différents. »

ITekia, entreprise intervenant dans la sécurité informatique depuis près de quinze ans, répond à ces exigences.

1.4 Contexte du rapport d'expertise

Le présent rapport correspond à l'expertise indépendante de la solution de vote électronique par Internet définie, réalisée et exploitée par la société NEOVOTE dans sa version et dans son implémentation prévue pour les élections des représentants au Conseil d'Administration au Conseil Académique, au Conseil de pôle humanités, au Conseil de pôle sociétés, au Conseil de pôle santé et au Conseil de pole sciences et technologie de l'Université de Nantes.

Cette expertise a été réalisée en novembre 2021 sur la base des spécifications de ce système et de son implémentation prévue en production. Elle est complétée par un audit de code et des tests d'intrusion.

L'analyse de code est destinée à s'assurer que le code source des applications déployées pour le système de vote répond correctement aux spécifications et qu'il ne comprend pas d'éléments de nature à présenter des risques et des vulnérabilités.

Les tests d'intrusion, conformément à la demande CNIL, sont un audit complémentaire destiné à s'assurer de la cohérence et de l'effectivité des solutions mises en œuvre.

La présente expertise consiste à s'assurer que toutes les dispositions, pertinentes pour la solution de vote, ont été prises afin de se conformer aux recommandations de la délibération CNIL 2019-053 de niveau 3 comme au décret n°2011-595.

Nota bene : la documentation recensée lors de l'expertise est conservée par le prestataire mettant en œuvre le système de vote compte tenu du caractère confidentiel des informations qui y figurent.

1.5 Limites de nos travaux

Les opinions indiquées dans ce rapport restent à apprécier dans des conditions normales ou raisonnablement prévisibles. Elles ne prennent notamment pas en compte les cas de force majeure.

2 Conclusions de l'expertise

Le système de vote électronique par Internet réalisé et mis en œuvre par le prestataire NEOVOTE dans sa version pour les élections des représentants au Conseil d'Administration au Conseil Académique, au Conseil de pôle humanités, au Conseil de pôle sociétés, au Conseil de pôle santé et au Conseil de pole sciences et technologie de l'Université de Nantes, et exploité conformément aux documents de référence de la version auditée, a été expertisé en regard de sa conformité aux recommandations de la Commission Nationale de l'Informatique et des Libertés délibération n°2019-053 du 25 avril 2019 relative à la sécurité des systèmes de vote électronique et au décret n°2011-595 .

L'Université nous a demandé, par précaution, d'analyser la conformité de son élection au niveau de risques le plus élevé de la délibération CNIL, à savoir le niveau de risques 3. Ce niveau de risques provient du résultat de la méthode d'identification du niveau de risques proposée par la CNIL dans sa fiche pratique sur le vote électronique.

De notre point de vue, selon les informations fournies par l'Université, le niveau de risques réel de ces élections serait 2, ce qui correspond au niveau de risques habituel des élections universitaires.

Nous affirmons en tant qu'expert en systèmes d'information qu'à notre connaissance, en fonction des éléments qui nous ont été transmis et communiqués (sous réserve que ces éléments soient sincères et véritables) et de l'expertise effectuée que le système de vote électronique ;

- **est globalement conforme aux dispositions relevant du niveau 3 de la Délibération CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique ; la principale conformité partielle identifiée réside dans l'usage possible du courrier électronique pour le retrait du mot de passe ce qui reste acceptable pour le niveau de risques de ces élections ;**
- **est conforme aux dispositions du décret n°2011-595 ;**
- **offre, en dehors de la faiblesse citée précédemment, un bon niveau de sécurité, correspondant au niveau attendu d'une solution de vote par Internet pour des scrutins de ce niveau de risques, aussi bien du point de vue technique que du point de vue des procédures organisationnelles encadrant sa mise en œuvre.**

A noter que nous n'avons pas connaissance de la réalisation d'une analyse de risques mais cette analyse de risques n'est demandé que pour les élections de niveau de risques 3, et n'est pas strictement nécessaire, selon notre opinion, dans le cadre de ces élections. En outre, l'absence de d'analyse de risques n'a pas d'impact sur la sincérité de ces élections.

Notre conclusion est basée sur les travaux menés dans le cadre de cette expertise et dont les résultats détaillés sont présentés dans les chapitres suivants de ce document.

Pour faire et valoir ce que de droit

Sébastien Roman

Expert – ITekia

Charols, le 18/11/2021

3 Contexte et organisation des élections

3.1 Organisation du scrutin

3.1.1 Le champ d'application

Les scrutins concernent les élections des représentants au Conseil d'Administration au Conseil Académique, au Conseil de pôle humanités, au Conseil de pôle sociétés, au Conseil de pôle santé et au Conseil de pole sciences et technologie de l'Université de Nantes. Plus précisément, les scrutins concernent les élections suivantes :

- Pour le Conseil d'administration :
  - 6 sièges pour le collège des professeurs des universités et personnels assimilés ; 6 sièges pour le collège des autres enseignants-chercheurs, des enseignants et personnels assimilés ; 5 sièges pour le collège BIATSS et 5 sièges pour le collège des usagers ;
- Pour le Conseil académique :
  - 20 sièges pour le collège des professeurs des universités et personnels assimilés ; 20 sièges pour le collège des autres enseignants-chercheurs, des enseignants et personnels assimilés ; 12 sièges pour le collège BIATSS et 18 sièges pour le collège des usagers ;
- Pour le Conseil de pôle Humanités :
  - 4 sièges pour le collège des professeurs des universités et personnels assimilés ; 4 sièges pour le collège des autres enseignants-chercheurs, des enseignants et personnels assimilés ; 4 sièges pour le collège BIATSS et 4 sièges pour le collège des usagers ;
- Pour le Conseil de pôle Sociétés :
  - 4 sièges pour le collège des professeurs des universités et personnels assimilés ; 4 sièges pour le collège des autres enseignants-chercheurs, des enseignants et personnels assimilés ; 4 sièges pour le collège BIATSS et 4 sièges pour le collège des usagers ;
- Pour le Conseil de pôle Santé :
  - 5 sièges pour le collège des professeurs des universités et personnels assimilés ; 5 sièges pour le collège des autres enseignants-chercheurs, des enseignants et personnels assimilés ; 5 sièges pour le collège BIATSS et 5 sièges pour le collège des usagers ;
- Pour le Conseil de pôle Sciences et Technologie :
  - 4 sièges pour le collège des professeurs des universités et personnels assimilés ; 4 sièges pour le collège des autres enseignants-chercheurs, des enseignants et personnels assimilés ; 4 sièges pour le collège BIATSS et 4 sièges pour le collège des usagers ;

La répartition des sièges est décrite dans l'arrêté électoral. Le vote s'effectue par voie électronique uniquement.

3.2 Les Bureaux de Vote Électronique

6 Bureaux de Vote Électronique (BVE) ont été constitués, à savoir un par instance.

Chaque bureau de vote comprend 1 président, 1 secrétaire et des délégués de liste, sauf pour le bureau de vote relatif au Conseil d'administration, qui ne comprend pas de secrétaire.

Les membres des bureaux de vote ont accès durant et à l'issue du scrutin, aux informations suivantes sur leur périmètre :

- aux listes électorales ;
- aux listes des candidats ;
- aux professions de foi des listes de candidats ;
- aux dates et horaires des scrutins ;
- aux compteurs des votes et taux de participation ;
- à la liste d'émargements ;
- au journal des évènements ;
- au code de scellement du système de vote.

3.3 Le Bureau de Vote Électronique Centralisateur

Un Bureau de Vote Électronique Centralisateur (BVEC), ayant la responsabilité de l'ensemble des scrutins, est constitué. Il comprend 1 président, 1 secrétaire et 4 délégués de liste.

Les membres du bureau de vote centralisateur ont accès durant et à l'issue du scrutin, aux informations suivantes sur l'ensemble des scrutins :

- aux listes électorales ;
- aux listes des candidats ;
- aux professions de foi des listes de candidats ;
- aux dates et horaires des scrutins ;
- aux compteurs des votes et taux de participation ;
- à la liste d'émargements ;
- au journal des évènements ;
- au code de scellement du système de vote.

Un fragment de la clé de chiffrement sera attribué à chaque membre du bureau de vote électronique centralisateur. Ces fragments seront générés lors de la cérémonie de scellement et remis aux porteurs. Le nombre minimum de fragments nécessaires pour dépouiller le vote est fixé à 3.

3.4 Transmission du matériel de vote

Le Prestataire adressera à chaque électeur un courrier électronique sur l'adresse institutionnelle, comprenant :

- Les dates et heures d'ouverture du scrutin ;
- L'adresse du site de vote et l'identifiant de l'électeur ;
- Une notice explicative sur les modalités du vote électronique.

L'électeur pourra à l'aide de son identifiant et d'une donnée personnelle, à savoir le numéro étudiant pour les usagers et le numéro de matricule pour les personnels, se connecter au site de vote afin de retirer son mot de passe. Ce mot de passe est ensuite envoyé à une destination qu'il fournit : numéro de portable pour les SMS, numéro de portable ou fixe pour un appel vocal.

Une assistance en ligne, accessible via la page de connexion du site de vote, peut également être utilisée pour demander la régénération des codes d'accès. Lors de cette demande, l'électeur devra saisir les deux premières lettres de son prénom, les quatre premières lettres de son nom de famille, sa donnée personnelle et un numéro de téléphone portable auquel il sera envoyé un SMS dont il faudra ressaisir le contenu.

3.5 Les postes dédiés

Des postes informatiques réservés au vote seront mis en place par l'Université de Nantes. Ces derniers se situent :

- Pôle Humanités / Pôle sociétés – TERTRE : Salle 63, RDC Aile A1, chemin de la Censive du Tertre, 44312 Nantes ;
- Pôle Santé : Bureau 144, 1er étage, 1 rue Gaston Veil, 44035 Nantes ;
- Pôle Sciences – MICHELET : Bâtiment 1, Amphi A, RDC, Université de Nantes 2 rue de la Houssinière, 44322 Nantes ;
- IUT Nantes (Fleuriaye) : Bureau F-D0/18, 2 avenue du Professeur Jean Rouxel, 44475 Carquefou ;
- IUT Nantes (Joffre) : Bureau J-A1/06, 3 rue du Maréchal Joffre, 44041 Nantes ;
- IUT Saint-Nazaire : Bâtiment 7, salle des professeurs (7, 130), 58 rue Michel Ange, 44600 Saint-Nazaire ;
- IUT La Roche-Sur-Yon : Salle de réunion n°109, RDC, Bâtiment B, 19 boulevard Gaston Defferre, 85000 La Roche-Sur-Yon ;
- INSPE Le Mans : Plot administration, RDC, 72 boulevard Pythagore, 72000 Le Mans ;
- INSPE Laval : 3 rue Georges Charpack, 53810 Change ;
- INSPE Angers : 49-9 rue Dacier, 49000 Angers ;
- INSPE Nantes : Hall, RDC, 44 chemin de Launay, 44000 Nantes ;
- Beaux-Arts : Salle R2, 038, 2ème étage – couloir administration, 2 allée Frida Kahlo, 44200 Nantes ;
- ENSA : Salle en face du service informatique, Bâtiment principal, étage 1B, 6 quai François Mitterrand, 44262 Nantes ;
- École Centrale : Bureau A120, Bâtiment A, 1 rue de la Noë, 44321 Nantes ;
- Halle 6 : Salle n°106, 1er étage, Halle 6 Ouest, 42 rue de la Tour d'Auvergne, 44200 Nantes ;
- Direction de la Formation Continue / Université Permanente (chantiers Navals) : 1er étage, Bureau n°118, Chantier Navals, 2 bis boulevard Léon Bureau, 44200 Nantes :
- Polytech : Bâtiment IHT, salle B016, RDC, rue Christian Pauc, 44306 Nantes.

3.6 L'accessibilité du site

La solution de vote électronique répond aux normes d'accessibilité du RGAA. En somme, elle est accessible à tout votant qu'il soit en situation de handicap ou non.

3.7 La cellule d'assistance technique

Une cellule d'assistance technique a été mise en place. Elle comprend :

- un représentant de la cellule des affaires institutionnelles ;
- un représentant de la direction des services juridiques ;
- le délégué à la protection des données ;
- le responsable sécurité informatique ;
- le chef de projet de NEOVOTE ;
- le directeur des opérations de NEOVOTE.

3.8 Le support électeur

Le prestataire de vote met en place un support électeur afin d'assister les électeurs pour ces élections. Il sera disponible 7 jours/7 et 24 heures/24 pendant les opérations de vote.

3.9 Les observateurs

Le scrutin comprendra les observateurs suivants : l'équipe technique de NEOVOTE et deux personnes désignées par l'organisateur des scrutins.

Les observateurs auront accès aux éléments suivants :

- aux listes électorales ;
- aux listes des candidats ;
- aux professions de foi des candidats ;
- aux dates et horaires des scrutins ;
- aux compteurs des votes et taux de participation ;
- à la liste des membres des bureaux de vote ;
- au journal des évènements ;
- au code de scellement du système de vote.

4 Présentation des travaux d'expertise

Les chapitres suivants présentent les résultats des travaux d'expertise menés par ITekia.

Nous avons délibérément choisi de présenter d'abord les résultats des travaux concernant la conformité aux objectifs de sécurité contenus dans la délibération CNIL n°2019-053. Cette délibération constitue l'interprétation de référence des dispositions législatives et réglementaires concernant les mesures à mettre en œuvre dans le cadre du recours au vote par voie électronique.

L'atteinte des objectifs de sécurité définis par la CNIL dans sa délibération n°2019-053 constitue donc le fondement sur lequel est basé notre opinion concernant l'atteinte des objectifs généraux décrits dans le décret n°2011-595.

4.1 Présentation des travaux d'analyse de conformité au regard de la délibération CNIL n°2019-053

En préambule du chapitre d'analyse détaillée à la délibération de la CNIL, nous présentons les éléments qui aux yeux de la CNIL, sont des préalables au recours au vote électronique, à savoir :

- la détermination du niveau de risques des élections ;
- le respect du règlement général de protection des données personnelles (RGPD) et notamment la réalisation d'une analyse d'impact sur la protection des données personnelles (AIPD) si le contexte le nécessite ;
- la fourniture d'une notice explicative aux électeurs.

Pour chacun des objectifs de sécurité de la délibération CNIL, nous rappelons d'abord l'objectif de sécurité tel qu'il est contenu dans la délibération.

Objectif n°X-0X : Énoncé de l'objectif de sécurité tel qu'il est contenu dans la délibération CNIL n°2019-053 parue au journal officiel le 21 juin 2019.

Afin d'aider les organisateurs de scrutins à bien comprendre ses attentes et d'éviter au maximum les ambiguïtés concernant les objectifs de sécurités, la CNIL a publié sur son site Internet une fiche pratique qui contient des exemples d'implémentation correctes de l'objectif de sécurité[3]. Ces exemples sont décrits sous la forme suivante :

Contenu de la fiche pratique fournie par la CNIL :

Rappel complet de l'exemple détaillé fourni par la CNIL

Nous décrivons ensuite les mesures mises en place dans le cadre de ces élections, avec leurs forces et leurs faiblesses. Enfin, nous exprimons notre conclusion concernant l'atteinte de l'objectif de sécurité sous la forme suivante :

Niveau de conformité :	**strictement conforme, conformité partielle mais acceptable, conformité insuffisante, non conforme selon le cas**
Ce texte exprime notre conclusion sous forme littérale et indique les principales raisons des éventuelles conformités partielles ou des non conformités.	

3 https://www.cnil.fr/fr/securite-des-systemes-de-vote-par-internet-la-cnil-actualise-sa-recommandation-de-2010

Chaque fois que nous estimons que le dispositif mis en place est partiellement conforme ou non conforme, nous en précisons, à notre avis, l'impact par rapport aux principes fondamentaux du droit électoral.

Impact de la conformité partielle : **Ce texte décrit les principaux impacts des non conformités ou des conformités partielles.**

4.2 Présentation des travaux d'analyse de conformité au regard du décret n°2011-595

Dans ces travaux, nous rappelons d'abord l'article ou l'alinéa du décret n°2011-595 concerné sous la forme suivante :

Alinéa X de l'article Y : Énoncé de l'alinéa tel qu'il est paru au journal officiel.

Nous décrivons ensuite les éléments qui nous permettent de justifier notre avis sur la conformité des mesures mises en place.

Enfin, nous exprimons un avis sur la conformité des mesures mises en œuvre sous cette forme :

Ce texte décrit notre avis sur la conformité des mesures mises en place au regard de l'alinéa analysé.

5 CONFORMITÉ A LA RECOMMANDATION 2019 DE LA CNIL

5.1 Exigences préalables

5.1.1 L'évaluation du niveau de risque du scrutin

Le niveau de risques de ces élections est évalué à 3 par l'organisateur du scrutin, conformément au résultat de la grille suivante :

	Vrai (0)	Faux (1)
Question 1 :Le scrutin peut être reporté, par exemple en cas d'incident.	0	
Question 2 : Le scrutin concerne moins de 50 personnes.		1
Question 3 : Le scrutin concerne moins de 1 000 personnes.		1
Question 4 : D'autres voies de vote sont possibles (à l'urne, à distance, etc.).		1
Question 5 :Les personnes élues n'ont pas de pouvoir décisionnel.		1
Question 6 : Les votants sont tous sur le territoire national.		1
Question 7 : Les votants sont tous sur le territoire européen.		1
Question 8 : Aucun élément laissant penser que le bon déroulement de l'élection puisse être affecté (menaces particulières, etc.) n'a été décelé.	0	
Question 9 : La validation du scrutin ne nécessite pas de preuves formelles de bon déroulé.		1
Question 10 : L'organisation du scrutin n'est pas une obligation légale.		1
Total		8

A noter que le niveau de risque 3 fourni par cette matrice, ne correspond pas à la définition donnée dans la délibération CNIL :

- *« Niveau 3 : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources importantes ou de fortes motivations. Ce niveau concerne les scrutins impliquant un nombre important d'électeurs et présentant un enjeu très élevé, dans un climat potentiellement conflictuel. Il s'agit par exemple d'élections de représentants du personnel au sein d'organisations importantes, à grande échelle et dans un cadre conflictuel. Le scrutin présente un risque important.»*

Au regard de votre contexte, nous sommes persuadé que vos élections sont de niveau 2, niveau de risques habituel des élections universitaires :

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

En outre, notre opinion est renforcée par le fait que le niveau 3 n'est atteint qu'en prenant en compte le faible nombre d'électeurs à l'étranger (Question 6 et 7).

L'organisateur des scrutins a néanmoins fait le choix de conserver un niveau de risques élevé, à savoir un niveau de risques 3. Nos conclusions prennent toutefois en compte que le niveau de risques reste modéré pour ces élections.

5.1.2 Analyse d'Impact relative à la Protection des Données Personnelles (AIPD)

L'organisateur du scrutin a réalisé une Analyse d'Impact relative à la Protection des Données Personnelles, qui n'a pas identifié de mesure de sécurité supplémentaire à mettre en place par rapport à celles déjà demandées dans la délibération CNIL n°2019-053 et le décret n° 2011-595.

5.1.3 Notice explicative fournie aux électeurs

Une notice explicative satisfaisante sur le fonctionnement du vote est fournie aux électeurs avec l'envoi du matériel de vote.

5.1.4 Objectifs de sécurité applicables

Des objectifs de sécurité sont associés à chacun des niveaux risques définis dans la délibération CNIL 2019-053. Il convient toutefois de noter que les objectifs sont cumulables, le niveau 2 étant composé d'objectifs de sécurité spécifiques et des objectifs de sécurité du niveau 1, le niveau 3 étant, quant à lui, composé d'objectifs de sécurité spécifiques et des objectifs de sécurité des deux niveaux précédents.

Le niveau de risques de ce scrutin étant classé à 3, il convient d'analyser le respect des objectifs de sécurité des niveaux 1, 2 et 3.

5.2 Conformité aux objectifs de sécurité du niveau de risques 1

5.2.1 Objectif de sécurité n° 1-01

Objectif n°1-01 : Mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers).

Contenu de la fiche pratique fournie par la CNIL :

« Utiliser les dernières versions stables et mises à jour des systèmes d'exploitation, des serveurs Web, des solutions de chiffrement et des bases de données mobilisées dans la solution. Il convient également d'utiliser des protocoles et algorithmes publics de chiffrement réputés « forts ».

Pour chaque élection, NEOVOTE recrée un nouveau système de vote à partir d'un modèle sous son contrôle.

Ce modèle est composé de 3 couches (ou 3 tiers dans le jargon informatique) :

- une couche applicative développée sous le contrôle exclusif de NEOVOTE dans le langage PHP ;
- une couche de base de données, basée sur l'utilisation de MySQL ;
- une couche de système d'exploitation basé sur le système d'exploitation Linux et plus particulièrement la distribution Debian.

Les couches de bases de données et de systèmes d'exploitation proviennent d'un éditeur tiers, à savoir la distribution Debian Linux, et donc font l'objet d'un suivi public de sécurité. C'est-à-dire que le projet Debian recense les éventuelles failles de sécurité, identifiées en interne, transmises confidentiellement par des tiers ou rendues publiques par ces mêmes tiers. Au fur et à mesure de la publication de la découverte de ce type de faille de sécurité, le projet Debian mets des correctifs de sécurité à disposition de ses utilisateurs.

Sur les systèmes de vote mis en œuvre par NEOVOTE, les mises à jour de la base de données comme des autres composants du système d'exploitation Debian sont gérés avec l'outil standard de gestion de paquets de Debian. C'est-à-dire qu'au moment du déploiement d'un nouveau système de vote, les versions déployées correspondent aux dernières versions fournies par la distribution, comprenant les correctifs de sécurité disponibles à la date de déploiement.

La couche applicable est réalisée spécifiquement par NEOVOTE. Le système de vote NEOVOTE est destiné à un usage exclusif dans le cadre des projets de vote mis en œuvre pour ses propres clients. Dans ces conditions, il n'existe pas de publications d'éventuelles failles de sécurité à destination de tiers qui utiliseraient le système de vote NEOVOTE.

Toutefois, l'application de vote de NEOVOTE a été auditée à de nombreuses reprises dans le cadre des expertises de vote électronique. Ces audits prennent la forme d'audit de code source et de tests d'intrusion d'un nombre significatif d'acteurs français du secteur de la sécurité des systèmes d'information.

Les faiblesses découvertes à l'occasion de ces audits sont prises en compte par NEOVOTE et font systématiquement l'objet d'une correction.

A la date de rédaction de ce rapport, nous n'avons identifié aucune faiblesse de sécurité dans les systèmes de vote mis en œuvre pour les élections des représentants au Conseil d'Administration au Conseil Académique, au Conseil de pôle humanités, au Conseil de pôle sociétés, au Conseil de pôle santé et au Conseil de pole sciences et technologie de l'Université de Nantes.

Par ailleurs, les algorithmes de chiffrement retenus par NEOVOTE dans le cadre de sa solution sont tous considérés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), comme des algorithmes « forts ». Plus précisément, il s'agit d'algorithmes recommandés dans l'Annexe B1 du Référentiel Général de Sécurité (RGS v2.0).

Le bulletin est chiffré avec l'algorithme RSA et une clé de 3072 bits. Toutes les empreintes cryptographiques sont réalisées à l'aide de l'algorithme de hachage SHA-256. Les nombres aléatoires sont générés à partir de générateurs aléatoires cryptographiquement sûrs. Selon le contexte d'usage de ces aléas, certains sont générés par l'API du navigateur de l'électeur, d'autres par le générateur aléatoire cryptographiquement sûr de PHP version 7.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.2.2 Objectif de sécurité n° 1-02

Objectif n°1-02 : Définir le vote d'un électeur comme une opération atomique, c'est-à- dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.

Contenu de la fiche pratique fournie par la CNIL :

« Dès lors que l'électeur a validé de manière définitive son choix de vote, l'ensemble des opérations précitées doit s'enchaîner sans discontinuité jusqu'à l'achèvement de la dernière action, c'est-à-dire jusqu'à la délivrance d'un récépissé. L'échec d'une action entraîne l'échec de toute la chaîne et, a contrario, la réussite de la chaîne n'est possible que de par le bon déroulement de chacune des actions unitaires. ».

Le choix et la validation du vote sont réalisés entièrement sur le terminal[4] de l'électeur. Plus précisément, le navigateur Internet de l'utilisateur récupère les différents choix de vote transmis par le système de vote. L'électeur peut alors sélectionner un ou plusieurs choix, dans les limites spécifiques des règles du scrutin concerné, et revenir en arrière autant de fois qu'il le désire tant qu'il n'a pas validé son vote.

Dans le cadre des élections de liste sans panachage, le choix de l'électeur se limite à choisir une des listes candidats ou le bulletin blanc qui lui est systématiquement proposé.

Tant que l'électeur n'a pas validé son choix, il lui est possible d'en changer. Pour valider son choix de vote, l'électeur doit entrer son mot de passe personnel qu'il a préalablement récupéré auprès du système de vote.

Une fois le choix de vote validé, l'expression du vote est mis en forme au travers d'un bulletin, qui est chiffré à l'aide de l'algorithme RSA et de la clé publique de l'élection. Ce bulletin chiffré est ensuite transmis au système de vote et accompagné des informations permettant d'identifier l'électeur qui a émis le bulletin.

A réception du bulletin, le système de vote procède à diverses vérifications d'usage telles que :

- est-ce que l'électeur est bien autorisé à voter sur le scrutin auquel il prétend participer ?
- a-t-il déjà voté ?
- le bulletin, sous forme chiffrée, est-il intègre ? c'est-à-dire est-ce qu'il a été modifié entre le terminal de l'électeur et le système de vote ?

Lorsque toutes les conditions sont réunies pour permettre le vote de l'électeur, le système de vote calcule un code qui fait office de récépissé de vote, procède à la mise à jour de l'émargement et au dépôt du bulletin dans l'urne.

A noter que la mise à jour de l'émargement et le dépôt du bulletin dans l'urne sont réalisés à travers une seule opération atomique. Dit autrement, un mécanisme de sécurité s'assure que l'émargement et le dépôt du bulletin chiffré sont complètement synchronisés : soit l'émargement est mis à jour et le bulletin déposé, soit l'émargement n'est pas mis à jour et le bulletin n'est pas ajouté dans l'urne.

Une fois que l'émargement et le bulletin chiffré sont bien enregistrés, le système de vote génère une preuve de vote puis retransmet à l'électeur le code faisant office de récépissé de vote et la preuve de vote.

La réalisation du vote par l'électeur comprend donc schématiquement les grandes étapes suivantes :

- étape 1 : le choix du vote ;
- étape 2 : la validation du vote par l'électeur et la génération d'un bulletin chiffré sur le terminal de l'électeur ainsi que la transmission de l'identité de l'électeur et du bulletin chiffré au système de vote ;
- étape 3 : la prise en compte du bulletin, la génération d'un code faisant office de récépissé de vote, la mise à jour de l'émargement et du bulletin de vote ;
- étape 4 : la génération de la preuve de vote ;
- étape 5 : le renvoi du code faisant office de récépissé et la preuve de vote.

4 Par terminal de l'électeur, il peut s'agir, selon le choix de chaque électeur, d'un smartphone, d'une tablette ou d'un ordinateur.

Les éventuelles défaillances techniques dans ce processus auraient des conséquences différentes selon l'étape où elles se produiraient :

- à l'étape 1 : l'électeur n'a pas encore validé son vote. Il est visible qu'il n'a pas voté ;
- à l'étape 2 ou à l'étape 3 : l'électeur a validé son vote, il pense avoir voté mais ne reçoit pas la confirmation de vote. Son vote n'est pas enregistré. L'électeur pourra revoter s'il se reconnecte ;
- à l'étape 4 ou à l'étape 5, le vote a bien été pris en compte. L'électeur ne reçoit pas immédiatement son récépissé de vote mais il peut prendre connaissance de l'accusé de réception de son vote en se reconnectant au système de vote.

Niveau de conformité :	**conformité partielle mais acceptable**

La solution mise en œuvre par NEOVOTE n'est pas strictement conforme aux attentes de la CNIL. A noter toutefois, que l'atteinte d'une conformité stricte nous paraît inatteignable[5].

La solution mise en œuvre est satisfaisante car sans impact réel sur la sincérité du scrutin.

Impact de la conformité partielle :

La probabilité d'une défaillance durant le temps très court de la procédure de vote reste très faible. Mais même en cas de défaillance, la sincérité du vote est préservée.

La solution mise en œuvre par NEOVOTE garantit la synchronisation entre l'urne et l'émargement. En outre, si une éventuelle défaillance apparaît avant la mise à jour de l'émargement et le dépôt du bulletin dans l'urne, l'électeur peut recommencer la procédure de vote et voter conformément à son choix.

Si une éventuelle défaillance apparaît entre l'enregistrement du vote et l'envoi du récépissé de vote, l'électeur peut récupérer son récépissé en se reconnectant au système de vote. Son choix de vote est correctement pris en compte.

5.2.3 Objectif de sécurité n° 1-03

Objectif n°1-03 : Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduits de manière significative.

Contenu de la fiche pratique fournie par la CNIL :

« L'électeur s'authentifie à l'aide d'un couple identifiant et mot de passe personnel qui lui a été remis de manière sécurisée (par deux canaux de communications séparés). Le fichier des électeurs comportant les éléments d'authentification est conservé de manière sécurisée. En cas de perte ou de vol de ses moyens d'authentification, une procédure permet à l'électeur d'effectuer son vote et rend les moyens d'authentification perdus ou volés inutilisables. ».

5 Le vote électronique implique 2 systèmes différents : le terminal de l'utilisateur et le système de vote. Nous ne connaissons aucune solution technique qui permettrait de répondre parfaitement aux attentes de la CNIL et d'implémenter une opération réellement atomique en impliquant plusieurs machines reliées par un réseau informatique.

L'électeur s'authentifie sur le système de vote à l'aide d'un identifiant personnel généré par le système de vote et d'une donnée personnelle (aussi appelée code défi), à savoir le numéro étudiant pour les usagers et le numéro de matricule pour les personnels.

Cet identifiant est transmis par courrier électronique à l'électeur sur son adresse institutionnelle. Une fois connecté, l'électeur pourra demander le retrait de son mot de passe. Celui-ci lui sera transmis, selon son choix, par mail, par SMS ou par appel vocal sur un numéro de son choix.

Afin de valider son vote, l'électeur devra utiliser son mot de passe.

A noter que la seule utilisation de l'identifiant, remis par courrier électronique et l'utilisation du numéro étudiant ou du numéro de matricule selon le cas, non transmis par le système de vote, suffit à répondre à cet objectif de sécurité de la CNIL.

Les données personnelles des utilisateurs sont conservées sous la forme d'une empreinte, générée à partir de 10 000 applications successives de l'algorithme SHA-256 au sein des serveurs de vote. Par ailleurs, le prestataire de vote conserve aussi ces données dans les serveurs utilisés pour le support électeur dans lesquels le stockage des données est sécurisé par un chiffrement AES-256

Le mot de passe est conservé de manière sécurisée avec un chiffrement AES-256 variabilisé par l'ajout de données aléatoires. Ce stockage par chiffrement et non pas par empreinte se justifie par le protocole de sécurisation global du transfert de l'enveloppe de vote décrit à l'objectif de sécurité n°1-05.

Les électeurs ont la possibilité de demander le renvoi de leur identifiant, notamment en s'adressant à l'assistance en ligne via le support en ligne ou le support téléphonique. Lors de cette demande, l'électeur devra saisir les deux premières lettres de son prénom, les quatre premières lettres de son nom de famille, sa donnée personnelle et un numéro de téléphone portable auquel il sera envoyé un SMS dont il faudra ressaisir le contenu.

A noter que le retrait du mot de passe comme le renouvellement du matériel de vote sont tracés, c'est-à-dire qu'ils génèrent un évènement visible dans le journal des évènements. Aussi, afin de restreindre les possibilités d'usurpation d'identité, les coordonnées utilisées pour retirer le mot de passe sont conservées par le système de vote et une même coordonnée (ie le numéro de téléphone) ne peut être utilisée pour retirer les mots de passe de plusieurs électeurs.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.2.4 Objectif de sécurité n° 1-04

Objectif n°1-04 : Assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant.

Contenu de la fiche pratique fournie par la CNIL :

« Chiffrer le bulletin sur le poste du votant, coté client et avant son émission, à l'aide d'un algorithme public réputé « fort ». »

La validation du choix de l'électeur déclenche la génération du bulletin de vote et son chiffrement.

Ce chiffrement est réalisé directement dans le terminal[6] de l'électeur au moyen de librairies javascript. L'algorithme utilisé est un algorithme asymétrique nommé RSA avec une clé de 3072 bits.

L'algorithme RSA est considéré comme un algorithme de chiffrement « fort » par l'Agence Nationale de la Sécurité des Systèmes d'Information. Elle recommande son utilisation pour la protection des secrets ne devant pas être connus avant 2030[7].

A noter que la génération de la clé est réalisée en utilisant le générateur aléatoire de la librairie OpenSSL, considéré comme cryptographiquement sûr.

Son envoi sécurisé au système de vote est assuré par un canal HTTPS. Toutes les traces du vote dans les fichiers temporaires ou permanents du terminal de l'électeur (un retour à l'écran précédent du navigateur ne donne aucune information) sont effacées.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.2.5 Objectif de sécurité n° 1-05

Objectif n°1-05 : Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.

Contenu de la fiche pratique fournie par la CNIL :

« Utiliser un canal sécurisé afin d'acheminer le bulletin, lui-même déjà chiffré (voir objectif de sécurité n° 1-02), du poste du votant jusqu'à l'urne électronique. Dans le cas de recours à des certificats, les choisir et les utiliser, au niveau 2, si possible conformément aux préconisations du RGS et, au niveau 3, conformément aux préconisations du RGS. »

6 Smartphone, tablette ou ordinateur
7 Référentiel Général de Sécurité (RGS v2) – Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Le bulletin est chiffré sur le terminal de l'électeur comme indiqué précédemment. Ce bulletin chiffré est transmis au sein d'un canal HTTPS, c'est-à-dire un canal lui-même chiffré par un des algorithmes de chiffrement forts décrits dans les versions 1.2 ou 1.3 du protocole TLS, selon les capacités du navigateur Internet.

Lorsque la version 1.2 du protocole TLS est employée, seuls sont utilisés les algorithmes de chiffrement conformes à la « Recommandations de sécurité relatives à TLS » publiée par l'Agence Nationale de la Sécurité des SI.

A noter que tous les algorithmes de chiffrement utilisables dans la version 1.3 de la norme TLS sont considérés comme des algorithmes de chiffrements forts et sont conformes à la même « Recommandations de sécurité relatives à TLS » publiée par l'ANSSI.

La confidentialité du bulletin durant son transport est donc garantie.

Le navigateur de l'électeur transmet une empreinte en même temps que le bulletin chiffré.

Cette empreinte est basée sur la concaténation du bulletin chiffré et du mot de passe qui, rappelons-le, est transmis par un canal différent (mail, SMS ou appel vocal selon le choix de l'électeur).

Le mot de passe n'est donc jamais transmis par le navigateur de l'électeur au système de vote. Une personne qui aurait découvert une éventuelle faille de sécurité dans la communication entre le navigateur et le système de vote, ne disposerait pas des informations lui permettant de générer cette empreinte.

A la réception du bulletin chiffré et de l'empreinte associée, le système de vote peut vérifier l'empreinte et donc l'intégrité du bulletin de vote chiffré.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.2.6 Objectif de sécurité n° 1-06

Objectif 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.

La fiche pratique fournie par la CNIL n'apporte aucune précision pour cet objectif de sécurité.

A réception d'un bulletin chiffré, celui-ci est déposé dans l'urne sans avoir été déchiffré. Il est conservé en l'état sans aucun déchiffrement avant le dépouillement.

A noter que pour dépouiller, il est nécessaire de posséder la clé secrète de l'élection. Cette clé secrète est bien générée sur le système de vote mais elle est effacée à l'issue de la séance de scellement et elle n'est reconstituée qu'au moment du dépouillement. Il n'est donc pas possible de prendre connaissance du contenu des bulletins avant le dépouillement.

Un contrôle d'intégrité de l'urne est réalisé dans un intervalle compris aléatoirement entre 1 et 59 secondes. Ce contrôle est basé sur la prise d'une empreinte de l'urne à l'aide de l'algorithme SHA-256 à chaque insertion de nouveau bulletin et à la clôture de l'urne.

A chaque fois qu'un nouveau bulletin chiffré est inséré dans l'urne, l'empreinte de l'urne est mise à jour. Ainsi, le système vérifie toutes les minutes que l'urne n'a pas fait l'objet d'une modification non autorisée.

Niveau de conformité :	**strictement conforme**

La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.

5.2.7 Objectif de sécurité n° 1-07

Objectif n°1-07 : Assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement.

Contenu de la fiche pratique fournie par la CNIL :

« Ne disposer d'aucun lien entre le votant et son bulletin chiffré dès lors que le vote est exprimé. Le bulletin n'est pas horodaté, contrairement à la liste d'émargement, et le bulletin et la liste sont conservés dans des espaces de stockage distincts. »

La séparation des données nominatives de l'électeur et l'expression de son vote est effective, dans le terminal, dès la validation du vote de l'électeur sur son terminal Internet ; elle est maintenue ensuite pendant tout le déroulement du scrutin.

Le système de vote reçoit en même temps l'identité du votant et son bulletin de vote chiffré. Il met alors à jour l'émargement et dépose le bulletin de vote chiffré dans l'urne.

L'émargement est horodaté et mis à jour dans l'ordre d'arrivée des bulletins. Cet émargement est stocké dans la base de données MySQL.

Les bulletins chiffrés sont placés dans un espace de stockage dédié. Chaque bulletin est rangé de manière complètement aléatoire dans une place libre de cet espace de stockage. Le générateur aléatoire utilisé est là encore le générateur aléatoire cryptographiquement sûr de PHP 7.

A noter que lors du dépôt de ce bulletin dans l'urne, un récépissé de vote et une preuve de vote sont générés.

Le récépissé de vote est un simple code correspondant à l'empreinte de l'émargement de l'électeur. Il permet de vérifier que l'électeur a bien voté mais ne contient aucune information sur son choix de vote. En cas de reconnexion au système de vote, l'électeur peut obtenir la régénération de son récépissé de vote.

Par contre, la preuve de vote permet à un électeur de retrouver son bulletin[8] comme le demande l'objectif de sécurité n°2-07 de la CNIL.

Cette preuve de vote est transmise à l'électeur et définitivement effacée du système de vote. En cas de reconnexion au système de vote, l'électeur ne peut pas obtenir la régénération de sa preuve de vote puisque qu'elle dépend du bulletin chiffré de l'électeur et que le système de vote est incapable d'identifier à qui appartient un bulletin déposé dans l'urne.

Le système de vote ne contient aucun lien ni temporel ni logique entre un émargement et un bulletin chiffré.

Niveau de conformité :	**strictement conforme**
Le système de vote assure une étanchéité totale entre l'identité de l'électeur et l'expression de son vote. Le seul lien entre l'électeur et son bulletin chiffré est en possession de l'électeur, dispositif mis en place afin de répondre à l'objectif de sécurité n°2-07 de la délibération CNIL n°2019-053.	

8 A partir de sa preuve de vote, l'électeur peut retrouver sa preuve de vote sous certaines réserves décrites à l'objectif n°2-07 de ce même rapport.

5.2.8 Objectif de sécurité n° 1-08

Objectif n°1-08 : Renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.

Contenu de la fiche pratique fournie par la CNIL :

« Générer a minima trois clés et exiger que deux de ces clés a minima soient indispensables afin de permettre le dépouillement. La génération des clés doit être réalisée de manière publique et ces dernières doivent être stockées sur un support sécurisé en possession uniquement du président du bureau et de ses assesseurs. »

Tous les bulletins des électeurs sont chiffrés sur le terminal de l'électeur à l'aide d'une clé publique. Le contenu de ces bulletins n'est accessible que pour le possesseur de la clé secrète de l'élection.

Cette clé secrète est générée au moment du scellement du système de vote, qui est réalisée en présence des membres du bureau de vote centralisateur, des membres des bureaux de vote et des observateurs.

Après sa génération, cette clé secrète est découpée en plusieurs fragments à l'aide de l'algorithme de Shamir. Chacun des fragments est attribué à un membre désigné du bureau de vote centralisateur au moment du scellement.

Dans le cadre de ces élections, l'organisateur du scrutin a choisi que les 6 membres du bureau de vote centralisateur seraient porteurs d'un fragment de la clé de chiffrement.

A noter qu'un membre du bureau de vote centralisateur se voit attribuer un et un seul fragment.

Ces porteurs de fragments ne reçoivent pas directement le fragment en clair de la clé secrète. Ces fragments sont protégés à l'aide de l'algorithme de chiffrement fort AES 256. Chaque fragment est protégé par une phrase secrète différente, générée par le système de vote, et transmise au porteur de ce même fragment.

Une fois que la clé secrète a été découpée, ses fragments chiffrés et les phrases secrètes transmises à leurs destinataires légitimes, la clé secrète de l'élection en clair, les fragments en clair de cette clé secrète et les phrases secrètes sont ensuite effacées du système de vote.

La clé secrète de l'élection est seulement reconstituée au dépouillement lorsqu'un nombre minimum de membres du bureau de vote centralisateur fournissent la phrase secrète en leur possession.

Dans le cadre de ces élections, ce nombre minimum est fixé à 3.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.2.9 Objectif de sécurité n° 1-09

Objectif n°1-09 : Définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin.

Contenu de la fiche pratique fournie par la CNIL :

« L'option de dépouillement ne doit être activable qu'après la fermeture du scrutin et le scellement de l'urne et de la liste d'émargement. L'opération de dépouillement, une fois activée, ne peut être interrompue avant d'être entièrement exécutée et terminée. Un dépouillement partiel ne peut ainsi être réalisé. »

Le dépouillement est une fonctionnalité qui n'est accessible, pour les membres du bureau de vote centralisateur, qu'à l'issue de la clôture du scrutin.

Aucun dépouillement partiel ne peut être réalisé avant la clôture du vote.

Au lancement du dépouillement, un nombre minimum de membres du bureau de vote centralisateur doit saisir sa phrase secrète comme indiqué dans l'objectif de sécurité précédent. Ces actions permettent la reconstitution de la clé secrète de l'élection sur le système de vote.

Le dépouillement réel des bulletins peut alors commencer. Les membres du bureau de vote centralisateur, les membres des bureaux de vote et les observateurs ne disposent alors d'aucune fonctionnalité leur permettant de stopper le dépouillement des bulletins qui se poursuit jusqu'à son terme, sauf éventuel incident.

Si un éventuel incident se produisait au cours du dépouillement, les résultats ne seraient pas fournis mais le dépouillement complet pourrait être relancé.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.2.10 Objectif de sécurité n° 1-10

Objectif n°1-10 Assurer l'intégrité du système, de l'urne et de la liste d'émargement.

Contenu de la fiche pratique fournie par la CNIL :

« S'assurer que le dispositif déployé est identique à celui audité par l'expert indépendant qui a effectué l'expertise commanditée par le responsable de traitement. Des empreintes des éléments doivent être calculées par l'expert et pouvoir être recalculées sur le système afin de les comparer et de les vérifier. L'urne et la liste d'émargement doivent être scellées et une empreinte calculée dès le scellement. »

Nous avons réalisé un audit du code source de la solution telle que demandée par la CNIL dans sa délibération n°2019-053.

A l'issue de cet audit, nous avons pris une empreinte du code source mais également de l'applicatif complet du système de vote. Cette prise d'empreinte est réalisée à l'aide de l'algorithme SHA-256. Cette empreinte[9] est visible en version longue et en version courte en annexe de ce rapport.

La version courte de l'empreinte est visible par les membres du bureau de vote centralisateur, les membres des bureaux de vote et les observateurs du scellement au dépouillement.

L'urne et la liste d'émargement sont constituées de données vivantes, c'est-à-dire que leur contenu est amené à évoluer en cours de scrutin et bénéficie donc d'un scellement dynamique.

A chaque fois qu'un bulletin est déposé dans l'urne, le système de vote calcule l'empreinte de celle-ci.

Le système de vote calcule d'abord l'empreinte d'un bloc de bulletins à l'aide de l'algorithme SHA-256. Il calcule ensuite l'empreinte de toutes les empreintes des blocs à l'aide du même algorithme SHA-256 et conserve cette empreinte.

Ainsi, la moindre modification du contenu entraîne un changement de l'empreinte de l'urne. Dit autrement, le système de vote peut refaire le calcul complet de l'empreinte et vérifier l'intégrité de l'urne.

La liste d'émargement bénéficie également d'un contrôle d'intégrité. Celui-ci est toutefois basé sur un chaînage cryptographique des émargements.

C'est-à-dire que lors du premier vote, le système calcule l'empreinte de l'émargement à l'aide de l'algorithme SHA-256. Ensuite, à chaque vote, le système de vote calcule l'empreinte cumulée de l'empreinte précédente et du nouvel émargement.

Cette empreinte cumulée est conservée par le système de vote afin de vérifier l'intégrité de la liste d'émargement.

De manière similaire au contrôle d'intégrité de l'urne, la moindre modification du contenu entraîne un changement de l'empreinte de la liste d'émargement, et l'intégrité de la liste d'émargement peut donc être vérifiée par le système de vote.

A noter que le calcul d'empreinte est réalisé de manière similaire sur le serveur principal et le serveur de secours. Ces empreintes doivent donc rester identiques sur les deux systèmes durant le scrutin.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.2.11 Objectif de sécurité n° 1-11

Objectif n°1-11 : S'assurer que le dépouillement de l'urne puisse être vérifié a posteriori.

Contenu de la fiche pratique fournie par la CNIL :

« L'option de dépouillement ne doit être activable qu'après la fermeture du scrutin et le scellement de l'urne et de la liste d'émargement. L'opération de dépouillement, une fois activée, ne peut être interrompue avant d'être entièrement exécutée et terminée. Un dépouillement partiel ne peut ainsi être réalisé. »

9 La version longue de l'empreinte consiste dans la suite de caractères hexadécimaux de l'empreinte et la version courte est constituée du résultat CRC32 de la version longue de cette empreinte.

A l'heure de clôture du vote, le système de vote clôt réellement le scrutin après un délai de grâce qui est paramétrable. C'est-à-dire que les électeurs qui se sont connectés avant l'heure de clôture disposent d'un délai de grâce pour terminer leur vote. Bien entendu, il n'est plus possible de se connecter au système de vote après l'heure de clôture du vote.

Lorsque le délai de grâce est atteint, le système de vote transfère les données de l'élection au coffre-fort électronique d'un tiers de confiance, à savoir l'Ofsad. Ces données sont sauvegardées sous forme chiffrée à l'aide d'une clé appartenant à NEOVOTE et spécifique à chaque prestation de vote.

Ainsi, le prestataire disposant du coffre-fort électronique ne dispose pas des données en clair de l'élection.

Cela concerne le paramétrage du système de vote, l'urne et la liste d'émargements, la clé publique de l'élection.

A noter qu'il n'est pas nécessaire de procéder à un scellement supplémentaire de la liste d'émargement et de l'urne, celles-ci font déjà l'objet d'un scellement dynamique depuis le scellement du système de vote.

Comme indiqué à l'objectif n°1-09, la fonctionnalité de dépouillement n'est accessible qu'après la clôture des scrutins et réalise le dépouillement de l'ensemble des scrutins.

La clé secrète de l'élection est également placée au coffre-fort électronique lorsqu'elle est reconstituée.

A l'aide des informations placées au coffre-fort électronique, il est possible de réaliser à nouveau un dépouillement des bulletins sous réserve qu'un nombre suffisant de membres du bureau de vote conserve leur phrase secrète.

La méthode à suivre consiste à :

- extraire du coffre-fort électronique les données de l'élection ;
- vérifier la signature de ces données afin de s'assurer qu'il s'agit bien des données des élections des représentants au Conseil d'Administration au Conseil Académique, au Conseil de pôle humanités, au Conseil de pôle sociétés, au Conseil de pôle santé et au Conseil de pole sciences et technologie ;
- déchiffrer ces données avec la clé secrète de NEOVOTE ;
- dépouiller les bulletins avec la clé secrète de l'élection ;
- procéder au recomptage des résultats.

Les programmes sources, les environnements d'exploitation et les fichiers de configuration sont sauvegardés par ailleurs et conservés sous la responsabilité du prestataire. A noter qu'une copie de ces programmes sources a été placée au coffre-fort électronique à l'issue de l'audit de celui-ci.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.3 Conformité aux objectifs de sécurité du niveau de risques 2

5.3.1 Objectif de sécurité n° 2-01

Objectif n°2-01 : Assurer une haute disponibilité de la solution.

Contenu de la fiche pratique fournie par la CNIL :

« Disposer d'une infrastructure dimensionnée pour supporter l'élection et la charge attendue. Il est prévu un système de redondance par un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et caractéristiques »

NEOVOTE met en place un système de vote qui comprend des machines plus ou moins puissantes en fonction du nombre d'électeurs.

Dans le cadre de ces élections, le système de vote est dit de taille 6. Il a fait l'objet d'une procédure de tests de charge, afin d'être en mesure de supporter l'éventualité où tous les électeurs voteraient.

En outre, le système de vote principal est déployé au sein du datacenter OVH de Gravelines qui bénéficie de moyens redondés :

- Au niveau réseau (firewall, commutateurs, liaisons opérateurs) ;
- Au niveau infrastructure (plusieurs serveurs physiques hébergeant machines virtuelles dédiées au vote).

Une supervision 24h/24 des infrastructures est réalisée.

Un système de vote de secours est installé au sein du datacenter OVH de Roubaix. Il bénéficie des mêmes mécanismes de protection que celui situé au sein du datacenter de Gravelines. Il est par défaut actif en permanence, ce qui permet de réceptionner une copie des bulletins chiffrés.

En cas de panne ou d'indisponibilité du système de vote principal, les électeurs sont automatiquement redirigés vers le système de vote de secours où ils peuvent voter dans les mêmes conditions que sur le système de vote principal.

Si le serveur principal redevenait actif, il se synchroniserait avec le serveur de secours afin de récupérer les bulletins et émargements qu'il n'aurait pas reçu durant le temps de son indisponibilité.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.3.2 Objectif de sécurité n° 2-02

Objectif n°2-02 : Assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement.

Contenu de la fiche pratique fournie par la CNIL :

« Calculer à intervalles non réguliers et non prévisibles une empreinte des éléments précités et les comparer à la valeur de référence calculée en amont (voir objectif de sécurité n° 1-08). »

Le contrôle d'intégrité de l'urne est réalisé en utilisant des empreintes réalisées avec l'algorithme SHA-256[10] tel que décrit à l'objectif de sécurité n°1-08.

Ce contrôle est réalisé à un intervalle aléatoire compris entre 1 et 59 secondes. Les résultats de ces contrôles sont visibles des membres du bureau de vote centralisateur et des membres des bureaux de vote qui peuvent exercer une surveillance effective du scrutin. Ils sont également visibles des observateurs.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.3.3 Objectif de sécurité n° 2-03

Objectif n°2-03 : Permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin.

Contenu de la fiche pratique fournie par la CNIL :

« Mettre à disposition du bureau électoral un dispositif lui permettant de vérifier directement la mise en œuvre de l'objectif de sécurité n° 2-02 depuis un écran de contrôle. »

Comme indiqué précédemment, les membres du bureau de vote centralisateur, les membres des bureaux de vote et les observateurs autorisés disposent d'une visualisation de l'état des contrôles d'intégrité dans leur espace de vote et d'un bouton permettant de déclencher à la demande une vérification.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.3.4 Objectif de sécurité n° 2-04

Objectif n°2-04 : Authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.

Contenu de la fiche pratique fournie par la CNIL :

« Solution 1 : L'électeur s'authentifie à l'aide d'un certificat électronique, choisi et utilisé conformément aux préconisations du RGS.

Solution 2 : L'électeur s'authentifie à l'aide d'un couple identifiant et mot de passe personnel qui lui a été remis de manière sécurisée (deux canaux séparés) et répond à une question défi-réponse non triviale (sont ainsi exclus la date de naissance et tout autre élément facilement décelable) dont il est le seul à connaître la réponse (avec le responsable de traitement). ».

10 Conforme aux recommandations de l'annexe B1 du Référentiel Général de Sécurité (RGS v2.0) publiée par l'Agence Nationale de la Sécurité des SI (ANSSI).

En cas de perte ou de vol de ses moyens d'authentification, une procédure permet à l'électeur d'effectuer son vote et rend les moyens d'authentification perdus ou volés inutilisables »

Il n'y a pas de recours à des données biométriques pour identifier l'utilisateur ni à des certificats de type RGSv2.

Comme indiqué à l'objectif de sécurité 1-03, les électeurs s'authentifient sur le système de vote à l'aide de leur identifiant et de leur donnée personnelle (aussi appelée code défi), à savoir le numéro étudiant pour les usagers et le numéro de matricule pour les personnels.

Cet identifiant, généré sur le système de vote, est transmis par courrier électronique aux électeurs sur leur adresse institutionnelle. Une fois connecté, l'électeur pourra demander le retrait de son mot de passe. Celui-ci lui sera transmis, selon son choix, par mail, par SMS ou par appel vocal sur un numéro de son choix.

Afin de valider son vote, l'électeur devra utiliser son mot de passe.

L'identifiant et le mot de passe sont générés sur le système de vote à l'aide d'un générateur aléatoire cryptographiquement sûr.

Les données personnelles choisies sont bien non triviales et leur connaissance restreinte à l'organisateur du scrutin et à l'électeur.

Les électeurs ont la possibilité de demander le renvoi de leur identifiant, notamment en s'adressant via le support en ligne ou le support téléphonique. Lors de cette demande, l'électeur devra saisir les deux premières lettres de son prénom, les quatre premières lettres de son nom de famille, sa donnée personnelle et un numéro de téléphone portable auquel il sera envoyé un SMS dont il faudra ressaisir le contenu.

A noter que le retrait du mot de passe comme le renouvellement du matériel de vote sont tracés, c'est-à-dire qu'ils génèrent un évènement visible dans le journal des évènements. Aussi, afin de restreindre les possibilités d'usurpation d'identité, les coordonnées utilisées pour retirer le mot de passe sont conservées par le système de vote et une même coordonnée (ie le numéro de téléphone) ne peut être utilisée pour retirer les mots de passe de plusieurs électeurs.

Niveau de conformité :	**conformité partielle mais acceptable**

L'attente de la CNIL correspond à un schéma d'authentification basé sur 3 éléments : un identifiant et un mot de passe, de bonne qualité et transmis par des canaux séparés ainsi qu'une donnée personnelle non-triviale qui n'est pas transmise par le système de vote à l'électeur.

Le mot de passe est transmis à une coordonnée, adresse de courrier électronique, SMS ou numéro de téléphone, librement choisie par l'électeur. Le système de vote ne peut donc pas vérifier que cette coordonnée correspond bien à une coordonnée utilisée par l'électeur.

Afin de limiter les possibilités de fraudes, une même coordonnée ne peut être utilisée pour plusieurs électeurs.

Impact de la conformité partielle :

La restriction de l'utilisation d'une même coordonnée par électeur a pour but de limiter les possibilités de fraudes mais cette règle reste peu efficace pour le retrait par courrier électronique saisit par l'utilisateur.

Le mécanisme d'authentification mis en œuvre est néanmoins d'un niveau correct, notamment au regard du canal employé pour distribuer l'identifiant et la robustesse de la donnée personnelle.

5.3.5 Objectif de sécurité n° 2-05

Objectif n°2-05 : Assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.

La fiche pratique fournie par la CNIL ne précise rien pour cet objectif de sécurité.

Le système de vote principal de ce scrutin est dédié, et lui-même contenu dans une machine virtuelle dédiée.

L'architecture du système de secours est identique.

Chacune de ces machines virtuelles sont déployées au sein d'infrastructures de gestion de ces mêmes machines virtuelles. Ce type d'infrastructure est spécifiquement conçu pour isoler les machines virtuelles et permettre une gestion complètement indépendante de celles-ci.

En l'état, l'arrêt d'une machine virtuelle dédiée à un scrutin pour un autre client du prestataire de vote n'aurait aucun impact sur le système de vote de ce scrutin.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.3.6 Objectif de sécurité n° 2-06

Objectif n°2-06 : Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.

Contenu de la fiche pratique fournie par la CNIL :

« Appliquer les bonnes pratiques mises en avant dans les documentations par les éditeurs, notamment les éditeurs de solutions de vote, mais également les éditeurs de serveur web, de serveurs d'application et les éditeurs de base de données. Appliquer, selon les cas d'espèce, les bonnes pratiques de l'ANSSI énoncées dans les guides « Recommandations pour la sécurisation des sites web », « Recommandations de sécurité relatives à TLS », « Recommandations de sécurité relatives à IPsec », « Recommandations de configuration d'un système GNU/Linux », « Recommandations de sécurité relatives à un système GNU/Linux », « Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows » et s'inspirer du document « La défense en profondeur appliquée aux systèmes d'information » et du guide d'hygiène. »

Le système de vote mis en œuvre par NEOVOTE n'utilise pas les technologies IPSec et Java, et n'est donc pas concerné par les recommandations de sécurité liées à ces technologies.

NEOVOTE a mis en place les bonnes pratiques recommandées dans le document « *Recommandations de sécurité relatives à TLS ».* Conformément aux recommandations de l'ANSSI, le système de vote n'accepte les communications chiffrées qu'avec la version 1.3 de TLS voire avec la version 1.2 de TLS sous réserve que le terminal de l'utilisateur supporte les algorithmes de chiffrement considérés comme forts.

NEOVOTE a mis en œuvre un premier niveau de renforcement de la sécurité de ses plateformes de vote. Ce durcissement a été renforcé afin de se conformer à tous les points de la « *Recommandations de configuration d'un système GNU/Linux ».* Un audit de la société ACCEISS a validé cette conformité.

Le système de vote est développé afin de respecter les bonnes pratiques recommandées par l'OWASP[11].

Le système de vote est également développé en séparant les fonctionnalités en plusieurs composants afin de mettre en œuvre les principes de défense en profondeur proposés par l'ANSSI[12].

En outre, les prestations d'infogérance des systèmes de vote réalisées par OVH rentrent dans un ensemble de prestations d'infogérance d'OVH bénéficiant d'une certification ISO 27001. Il s'agit d'une certification concernant la gestion de la sécurité. Elle impose notamment de réaliser régulièrement des états des lieux de son niveau de sécurité afin de s'assurer de l'adéquation de ses pratiques en matière de sécurité avec ses besoins.

Enfin, le système de vote est bâti afin de respecter les préconisations de l'ANSSI concernant les mécanismes cryptographiques, à savoir l'annexe B1 du Référentiel Général de Sécurité.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.3.7 Objectif de sécurité n° 2-07

Objectif n°2-07 : Assurer la transparence de l'urne pour tous les électeurs.

Contenu de la fiche pratique fournie par la CNIL :

L'exemple fournit par la CNIL est le suivant :

« Rassurer autant que possible les votants qui n'ont pas accès à l'expertise de la solution de vote, garante du bon fonctionnement du dispositif et de la sincérité et intégrité du vote dans son ensemble. Il s'agit de permettre aux électeurs de s'assurer que leur bulletin a été pris en compte dans l'urne et que les bulletins de vote sont construits de manière correcte.

Pour ce faire :

Chaque récépissé de vote contient une information unique, totalement décorrélée de l'identité du votant (empreinte numérique, numéro aléatoire, « preuve à divulgation nulle de connaissance », etc.) qui est calculée au moment où le votant valide son choix de vote. La plateforme de vote électronique est destinataire de l'information et la publie afin de la rendre accessible à tous les électeurs. Chaque électeur peut ainsi avoir la garantie que son bulletin est bien dans l'urne.

De plus, la solution de vote permet aux votants d'accéder à un espace de test où il est possible d'effectuer différents votes de tests et de voir ce qui ressort de l'ouverture du bulletin sur le serveur, le but étant de s'assurer que les bulletins sont correctement construits. »

NEOVOTE fait montre de transparence en fournissant tout le support nécessaire permettant la réalisation d'expertises indépendantes de son système de vote. Cela comprend en particulier :

- L'accès au code source de son système de vote ;
- La fourniture de documentation sur son implémentation ;
- La possibilité de réaliser des tests d'intrusion de la plateforme.

11 Open Web Application Security Project (OWASP) est une communauté internationale d'expert définissant des guides d'audit et de développement sécurisés d'application Web. Régulièrement, ils publient également la liste des vulnérabilités les plus fréquentes des sites Web. Cette liste est connue sous le nom Top Ten OWASP.
12 La défense en profondeur appliquée aux systèmes d'information - ANSSI

Lors de la phase de vote, le navigateur du votant chiffre le bulletin de vote, calcule une empreinte de celui-ci, mémorise cette empreinte et transmet le bulletin de vote chiffré au serveur.

Le serveur de vote stocke aléatoirement l'enveloppe de vote dans l'urne. Il collecte dans l'urne les empreintes de 4 bulletins choisis aléatoirement dans le même scrutin.

A noter que pour les quatre premiers électeurs, ces empreintes de bulletins sont remplacées par de l'aléa constituant quatre fausses empreintes de bulletins identifiées comme tels.

Le système de vote mélange ensuite ces 5 empreintes, les concatène et ajoute un sel aléatoire. Il ajoute également une somme de contrôle. Le serveur chiffre cette chaîne à l'aide de l'algorithme AES et renvoie le tout au navigateur de l'électeur.

Le navigateur de l'électeur qui dispose en JS de la clef AES, déchiffre la preuve de vote et vérifie qu'elle contient bien l'empreinte du bulletin tel que calculé en local avant envoi. En cas d'incohérence, un message d'alerte est affiché à l'électeur et un message est envoyé à l'équipe technique de NEOVOTE. En cas de succès, le navigateur affiche au votant sa preuve de vote et lui propose de la conserver via téléchargement ou copier-coller.

En outre, l'électeur pourra vérifier sa preuve de vote sur un système mis à disposition chez un huissier.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.4 Conformité aux objectifs de sécurité du niveau de risques 3

5.4.1 Objectif de sécurité n° 3-01

Objectif n°3-01 : Étudier les risques selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte de mise en œuvre.

La fiche pratique fournie par la CNIL n'apporte pas de précisions pour cet objectif de sécurité.

La réalisation d'une analyse de risques comprend l'étude des menaces pesant sur le vote. A notre connaissance, ce type d'étude n'a pas été réalisée dans le cadre de ces élections.

Niveau de conformité :	**conformité partielle mais acceptable**
Nous ne disposons pas d'une analyse de risques propre à ces élections.	

Impact de la conformité partielle :

Selon notre opinion, ces scrutins sont seulement de niveau 2, l'absence d'analyse de risques n'entraîne donc aucun impact sur la sincérité du vote.

5.4.2 Objectif de sécurité n° 3-02

Objectif n°3-02 : Permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers

Contenu de la fiche pratique fournie par la CNIL :

«Procéder de la même manière que pour l'objectif de sécurité n°2-07 en effectuant de surcroît les vérifications sur une machine tierce, mise en œuvre par un partenaire externe au vote. »

La société NEOVOTE a conclu un accord avec un huissier afin qu'il puisse mettre à disposition une solution de vérification de l'urne.

Cette solution est accessible aux électeurs, après le dépouillement du scrutin, à l'URL suivante : https://www.verifier-mon-vote.fr/. A l'issue de l'élection, ils pourront soumettre leur preuve de vote à cette application qui leur fournira une liste de 5 votes existants dont l'un d'eux correspond à leur bulletin.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.4.3 Objectif de sécurité n° 3-03

Objectif n°3-03 : Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.

Contenu de la fiche pratique fournie par la CNIL :

« Disposer d'une infrastructure dimensionnée pour supporter la charge attendue induite par le processus électoral. Il est prévu un système de redondance par un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et caractéristiques. Prévoir une redondance de l'alimentation de chaque machine, ainsi que des accès à Internet de l'infrastructure. Les sites hébergeant l'infrastructure principale et de secours doivent être suffisamment distants et correctement placés afin de couvrir les risques naturels. »

La solution NEOVOTE comprend un serveur principal et un serveur de secours. Ces éléments sont répartis sur deux sites géographiquement distincts (Roubaix d'un coté, et Gravelines de l'autre).

Le serveur principal et le serveur de secours disposent des mêmes mécanismes de sécurité. En outre, le bulletin chiffré est systématiquement enregistré sur les deux serveurs. En cas de défaillance d'un des deux serveurs, le vote peut continuer sans interruption sur le second serveur.

Enfin, un troisième serveur, dit serveur PRA, permet d'enregistrer les votes si le serveur principal ou le serveur de secours sont défaillants. C'est-à-dire que les bulletins sont systématiquement enregistrés sur 2 serveurs. Lorsque le serveur défaillant revient, il se synchronise avec le serveur PRA afin de récupérer les bulletins manquants.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.4.4 Objectif de sécurité n° 3-04

Objectif n°3-04 : Permettre le contrôle automatique et manuel par le bureau de vote de l'intégrité de la plateforme pendant tout le scrutin.

Contenu de la fiche pratique fournie par la CNIL :

« Donner la possibilité au bureau de vote de déclencher manuellement un contrôle de l'intégrité de la plateforme en supplément du contrôle automatique énoncé par l'objectif n°2-03. »

Le calcul d'intégrité est réalisé en moyenne toutes les 30 secondes et ce résultat est affiché dans l'interface des membres du bureau de vote. Durant toute la durée du scrutin, un contrôle automatique est réalisé et permet donc au bureau de vote de vérifier l'intégrité de la plateforme.

En outre, le bureau de vote dispose d'un bouton lui permettant de rejouer immédiatement le contrôle d'intégrité et donc de s'assurer manuellement de l'intégrité de la plateforme.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

5.4.5 Objectif de sécurité n° 3-05

Objectif n°3-05 : Assurer un cloisonnement physique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.

La fiche pratique fournie par la CNIL n'apporte pas de précisions pour cet objectif de sécurité.

Le serveur principal comme le serveur de secours sont des machines virtuelles dédiées pour chaque élection. Ces machines virtuelles sont hébergées au sein de machines dédiées au vote électronique.

L'arrêt du serveur principal comme du serveur de secours est possible et sans impact sur le fonctionnement des autres machines virtuelles fonctionnant sur les mêmes machines.

Niveau de conformité :	**strictement conforme**
La solution mise en œuvre par NEOVOTE est satisfaisante par rapport à l'objectif de sécurité.	

6 Conformité au décret n°2011-595

6.1 Article 2

Alinéa 1 de l'article 2 : Le vote électronique par internet peut constituer la modalité exclusive d'expression des suffrages ou constituer l'une de ces modalités.

Le vote électronique constitue la modalité exclusive du vote conformément à la possibilité offerte par l'alinéa de cet article.

Alinéa 2 de l'article 2 : Le recours au vote électronique par Internet est organisé dans le respect des principes fondamentaux qui commandent les opérations électorales, notamment la sincérité des opérations électorales, l'accès au vote de tous les électeurs, le secret du scrutin, le caractère personnel, libre et anonyme du vote, l'intégrité des suffrages exprimés, la surveillance effective du scrutin et le contrôle a posteriori par le juge de l'élection.

Afin de vérifier le respect par le système de vote des principes fondamentaux qui commandent les opérations électorales, nous avons vérifié la mise en œuvre des mesures identifiées par la CNIL afin de répondre à ces dispositions législatives et réglementaires.

En particulier, le système de vote est accessible à tous les électeurs par le terminal de leur choix. S'ils ne disposent pas d'un poste informatique, des postes en libre-service sont disponibles.

Le système de vote NEOVOTE met en œuvre les mesures de sécurité concernant le chiffrement du bulletin, via des mécanismes réputés forts et son stockage sécurisé. A aucun moment, le secret d'un vote exprimé par l'électeur ne peut être levé sans la participation active de l'électeur, qui lève le secret lié à son propre vote.

L'électeur se voit proposer l'ensemble des choix de vote disponible pour son collège, y compris le vote blanc. Le système de vote accepte de la même manière tous les bulletins qui correspondent à l'un des choix proposés.

Les membres du bureau de vote centralisateur et les membres des bureaux de vote disposent des moyens de réaliser une surveillance effective des scrutins, notamment en disposant des moyens de contrôler l'intégrité de la plateforme de vote et le contenu de la liste d'émargement.

Le contrôle a posteriori de l'élection est possible, en récupérant les données enregistrées au sein du coffre-fort électronique.

Le lien entre l'électeur et l'expression de son vote est rompu lors de la mise à jour de l'émargement et le dépôt du bulletin dans l'urne.

L'électeur est le seul à disposer d'un lien, toutefois indirect, vers l'expression de son vote, qui plus est sous forme chiffrée. Cette fonctionnalité est mise en place afin de répondre à l'objectif de transparence de l'urne demandée par la CNIL.

6.2 Article 3

Alinéa 2 de l'article 3 : Chaque scrutin propre à une instance de représentation des personnels donne lieu à la constitution d'un bureau de vote électronique.

En outre et en tant que de besoin, peuvent être créés des bureaux de vote électronique centralisateurs ayant la responsabilité de plusieurs scrutins. Ces bureaux comprennent un président et un secrétaire désignés par l'autorité administrative ainsi que les délégués de liste.

En cas de coexistence de plusieurs modalités d'expression des suffrages pour un même scrutin, le bureau de vote électronique tient lieu de bureau de vote central.

Les scrutins ont donné lieu à la constitution de 6 bureaux de vote et d'un bureau de vote centralisateur ayant la responsabilité de l'ensemble des scrutins.

Le bureau de vote électronique centralisateur est composé d'un président, d'un secrétaire et de 4 délégués de liste.

Alinéa 3 de l'article 3 : La conception, la gestion et la maintenance du système de vote électronique par internet peuvent être confiées à un prestataire choisi par l'administration sur la base d'un cahier des charges respectant les dispositions du présent décret et des arrêtés ou décisions mentionnés à l'article 5.

L'organisateur du scrutin, à savoir l'Université de Nantes, a choisi de recourir au prestataire de vote NEOVOTE pour la réalisation de ses élections par voie électronique.

Ce prestataire a été sélectionné sur la base d'un cahier des charges défini par l'Université de Nantes.

Alinéa 4 de l'article 3 : L'administration met en place une cellule d'assistance technique chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique. Cette cellule comprend des représentants de l'administration, ainsi que, lorsqu'il est recouru à un prestataire, des préposés de celui-ci.

L'Université de Nantes a bien mis en œuvre une cellule d'assistance technique comprenant :

- un représentant de la cellule des affaires institutionnelles ;
- un représentant de la direction des services juridiques ;
- le délégué à la protection des données ;
- le responsable sécurité informatique ;
- le chef de projet de NEOVOTE ;
- le directeur des opérations de NEOVOTE.

Alinéa 5 de l'article 3 : Les obligations de confidentialité et de sécurité mentionnées au premier alinéa du I de l'article 4 s'imposent à l'ensemble des personnes intervenant sur le système de vote électronique par internet, notamment aux agents de l'administration chargés de la gestion et de la maintenance du système de vote et à ceux du prestataire, si ces opérations lui ont été confiées.

Le prestataire de vote respecte un engagement de confidentialité et notamment le Règlement Général sur la Protection des Données.

6.3 Article 4

Alinéa 1 de l'article 4 : Les systèmes de vote électronique par internet comportent des mesures physiques et logiques permettant d'assurer la confidentialité des données transmises, notamment la confidentialité des fichiers constitués pour établir les listes électorales, ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

Les fonctions de sécurité des systèmes de vote électronique par internet doivent être conformes au référentiel général de sécurité prévu à l'article 9 de l'ordonnance du 8 décembre 2005 susvisée.

Le système de vote est déployé au sein de datacenters de la société OVH, qui met en œuvre les mesures de sécurité nécessaires afin d'assurer la protection physique des machines hébergeant les systèmes de vote. La réalité des pratiques de sécurité de la société OVH est attestée par l'obtention d'un certificat ISO 27001 concernant sa gestion de la sécurité des plateformes hébergées.

NEOVOTE a mis en œuvre les bonnes pratiques de sécurité logiques telles que décrites à l'objectif de sécurité n°2-06 de la délibération n°2019-053 de la CNIL.

NEOVOTE met également en œuvre les recommandations de la CNIL concernant l'authentification des électeurs, l'émargement, l'enregistrement et le dépouillement des votes.

En outre, la société NEOVOTE a signé un engagement de confidentialité concernant les intervenants sur ses plateformes de vote.

Les mesures prises sont conformes aux fonctions de sécurité décrites dans le Référentiel Général de Sécurité (RGS) v1.0 prévu à l'article 9 de l'ordonnance du 8 décembre 2005. Les algorithmes mis en œuvre par la solution sont conformes à l'annexe B1 du RGS v2.0, actuellement en vigueur.

Alinéa 2 de l'article 4 : Les données relatives aux électeurs inscrits sur les listes électorales ainsi que les données relatives aux votes dont l'objet de traitements informatiques distincts, dédiés et isolés, respectivement dénommés « fichier des électeurs » et « contenu de l'urne électronique ».

En cas de recours à un même système de vote pour plusieurs scrutins, chacun de ces scrutins doit être isolé sur un système informatique dépendant.

Les données relatives aux électeurs inscrits sur les listes électorales ainsi que les données relatives aux votes font l'objet de traitements informatiques distincts, dédiés et isolés, respectivement dénommés « liste d'émargements » et « urne électronique ».

Conformément à l'objectif de sécurité n°2-05 de la délibération CNIL, chaque prestation de vote est isolée sur un système informatique indépendant.

Alinéa 3 de l'article 4 : Chaque système de vote électronique par internet comporte un dispositif de secours offrant les mêmes garanties et les mêmes caractéristiques que le système principal et capable d'en prendre automatiquement le relais en cas de panne n'entraînant pas d'altération des données.

NEOVOTE a mis en œuvre un serveur principal et un serveur de secours pour ces élections. Ces serveurs bénéficient de la même configuration applicative et des mêmes mesures de protection physique.

Il sont placés dans des datacenters distincts, distants d'une centaine de kilomètres.

Le système de secours et le système principal sont actifs en permanence. Tant que les deux sont actifs, ils se synchronisent en permanence afin que chacun d'eux dispose des mêmes données sur les votes en cours. En cas de défaillance du système principal, les électeurs sont automatiquement redirigés vers le système de vote de secours.

6.4 Article 7

Article 7 : Préalablement à la mise en place ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties prévues par le présent décret. Cette expertise couvre l'intégralité du dispositif installé avant le scrutin, les conditions d'utilisation du système de vote durant le scrutin, les conditions d'utilisation du poste dédié mentionné au II de l'article 9 ainsi que les étapes postérieures au vote.

Le rapport de l'expert est transmis par l'administration à la Commission Nationale de l'Informatique et des Libertés et aux organisations syndicales ayant déposé une candidature au scrutin.

Le système de vote a fait l'objet d'une expertise préalable, décrite dans ce rapport. Il appartient à l'organisateur du scrutin de transmettre ce rapport à la Commission Nationale de l'Informatique et des Liberté ainsi qu'aux organisations syndicales ayant déposé une candidature au scrutin.

6.5 Article 8

Article 8 : Les membres des bureaux de vote et, le cas échéant, des sections de vote, y compris les délégués de liste, bénéficient d'une formation sur le système de vote électronique qui sera utilisé. Les documents de présentation y afférents leur sont communiqués.

L'administration met en place un centre d'appels chargé de répondre aux questions des électeurs pendant toute la période de vote et selon des modalités et des horaires fixées par l'arrêté ou la décision prévus à l'article 5.

Les membres du bureau de vote centralisateur et les membres des bureaux de vote bénéficient d'un test à blanc, tenant lieu de formation, qui est dispensé avant le scellement du système de vote.

Le centre d'appel, mis en place par le prestataire de vote, est en charge de répondre aux demandes des électeurs.

6.6 Article 9

Alinéa 2 de l'article 9 : L'électeur a la possibilité d'exprimer son vote par internet sur un poste dédié dans un local aménagé à cet effet, situé dans les services de l'administration concernée et accessible pendant les heures de service. L'administration s'assure que les conditions nécessaires à l'anonymat, la confidentialité et le secret du vote sont respectées.

L'arrêté ou la décision mentionnés au I fixent la durée de mise à disposition des postes dédiés. Cette durée ne peut être inférieure à deux jours lorsque la période durant laquelle le vote électronique est ouvert est supérieure à deux jours. Dans le cas contraire, elle ne peut être inférieure à une journée.

Des postes dédiés à cet effet seront mis à disposition. Leur localisation est décrite au point 3.5 du présent rapport. Ils seront accessibles pendant toute la durée du vote.

6.7 Article 10

Article 10 : Chaque électeur reçoit au moins quinze jours avant le premier jour du scrutin une notice d'information détaillée sur le déroulement des opérations électorales et un moyen d'authentification lui permettant de participer au scrutin. Ce moyen d'authentification lui est transmis selon les modalités garantissant sa confidentialité.

Les moyens d'authentification appropriés sont mis en œuvre par le système de vote. Ils sont conformes aux attentes de la délibération CNIL n°2019-053.

Ils comprennent l'envoi des moyens d'authentification aux électeurs accompagnés d'une notice explicative.

6.8 Article 11

Alinéa 1 de l'article 11 : Avant le début des opérations de scellement, il est procédé, sous le contrôle de l'administration à des tests du système de vote électronique et du système de dépouillement.

Le système fait l'objet d'un test préalable aux opérations de vote par les membres du bureau de vote centralisateur et les membres des bureaux de vote avant l'opération de scellement.

Alinéa 2 de l'article 11 : Avant le début du scrutin, le bureau de vote électronique : 1° Procède à l'établissement et à la répartition des clefs de chiffrement mentionnées au III ; 2° Vérifie que les composantes du système de vote électronique ayant fait l'objet d'une expertise n'ont pas été modifiées et s'assure que les tests prévus au I ont été effectués ; 3° Vérifie que l'urne électronique est vide, scellée et chiffrée par des clefs de chiffrement délivrées à cet effet ; 4° Procède au scellement du système de vote électronique, de la liste des candidats, de la liste des électeurs, des heures d'ouverture et de fermeture du scrutin ainsi que du système de dépouillement. La séance au cours de laquelle il est procédé à l'établissement et à la répartition des clefs de chiffrement est ouverte aux électeurs.

Les clefs de scellement sont réparties entre les membres du bureau de vote électronique centralisateur. Ils sont désignés sous le terme de « porteurs » des fragments de clés de l'élection.

Les membres du bureau de vote centralisateur et les membres des bureaux de vote disposent de l'accès au système de vote et peuvent vérifier l'empreinte du système de vote. Il peuvent également vérifier que l'urne est vide avant de sceller le système.

Alinéa 3 de l'article 11 : Les modalités d'établissement et de répartition des clés de chiffrement sont précisées par l'arrêté ou la décision prévus à l'article 5 dans le respect des conditions suivantes :

1° Au moins trois clés de chiffrement sont éditées et attribuées à des membres du bureau de vote électronique ;

2° Au moins deux tiers des clés éditées sont attribuées aux délégués de liste et au moins une clé est attribuée au président du bureau de vote ou à son représentant ;

3° Chaque clé est attribuée selon une procédure garantissant aux attributaires qu'ils ont, seuls, connaissance du mot de passe associé à la clé qui leur est personnellement attribuée, cette garantie s'imposant y compris à l'égard du personnel technique chargé du déploiement du système de vote électronique ;

4° Le scellement prévu au 3° du II est effectué par la combinaison d'au moins deux clés de chiffrement, dont celle du président du bureau de vote ou de son représentant et celle d'au moins un délégué de liste.

Le nombre de fragments de clés de chiffrement prévus est égal au nombre de membres du bureau de vote centralisateur dont 3 permettent de retrouver la clé secrète des élections et de dépouiller. Les mots de passe protégeant ces clés sont générés par le système.

Le mot de passe protégeant un fragment de clé est uniquement transmis par clé USB au porteur du fragment concerné. Chacun des « porteurs » de clés de l'élection ne possède donc qu'un fragment de clés de chiffrement.

6.9 Article 12

Alinéa 1 de l'article 12 : Durant la période de déroulement du scrutin, la liste d'émargement et l'urne électronique font l'objet d'un procédé garantissant qu'elles ne peuvent être modifiées respectivement que par l'ajout d'un émargement et par l'ajout d'un bulletin qui émanent d'un électeur authentifié dans les conditions prévues à l'article 13 et dont l'intégrité est assurée.

La liste d'émargement et l'urne font l'objet d'un contrôle d'intégrité.

Toute modification de l'urne ou de la liste d'émargement de manière non autorisée serait détectée.

Alinéa 2 de l'article 12 : Durant la même période :

1° Les fichiers comportant les éléments d'authentification des électeurs et le contenu de l'urne sont inaccessibles ;

2° La liste d'émargement et le compteur des votes ne sont accessibles qu'aux membres du bureau de vote à des fins de contrôle du déroulement du scrutin ;

3° Aucun résultat partiel ne peut être comptabilisé.

Le système de vote fait l'objet d'un isolement qui le rend accessible seulement à travers les interfaces du système de vote.

Les fichiers contenant les éléments d'authentification des électeurs et le contenu de l'urne sont inaccessibles, y compris pour les équipes techniques de NEOVOTE.

Une procédure existe pour rompre l'isolement du serveur et permettre les interventions de l'équipe technique en cas de situation d'urgence. Toutefois, la rupture de cette isolement est tracée et visible par les membres du bureau de vote centralisateur et les membres des bureaux de vote.

La liste d'émargement n'est accessible qu'aux membres du bureau de vote.

Aucun résultat partiel ne peut être comptabilisé.

Alinéa 3 de l'article 12 : Les interventions sur le système de vote sont réservées aux seules personnes chargées de la gestion et de la maintenance mentionnées à l'article 3 et ne peuvent avoir lieu qu'en cas de risque d'altération des données. Les bureaux de vote sont immédiatement tenus informés des interventions techniques sur le système de vote ainsi que des mesures prises pour remédier au dysfonctionnement ayant motivé l'intervention.

Seuls les intervenants de NEOVOTE peuvent accéder aux systèmes de vote, et seulement après avoir rompu l'isolement du serveur.

Les procédures de NEOVOTE impliquent que l'organisateur du scrutin soit prévenu avant toute intervention.

La rupture de l'isolement est immédiatement visible dans l'interface des membres du bureau de vote centralisateur et des membres des bureaux de vote. Ce changement ne peut pas être effacé.

En outre, les interventions sont tracées.

6.10 Article 13

Alinéa 1 de l'article 13 : Pour se connecter au système de vote, l'électeur doit s'identifier par le moyen d'authentification qui lui a été transmis. Ce moyen d'authentification permet au serveur de vérifier l'identité de l'électeur et interdit à quiconque de voter de nouveau pour le même scrutin avec le même moyen d'authentification.

Les moyens d'authentification utilisés sont globalement conformes aux attentes de la CNIL et permettent de réduire significativement les risques d'usurpation d'identité.

Alinéa 2 de l'article 13 : L'électeur a accès, selon son cas, aux listes de candidats ou aux sigles des organisations syndicales candidates, lesquels doivent apparaître simultanément à l'écran. Le vote blanc est possible.

L'électeur est invité à exprimer son vote. Le vote doit apparaître clairement à l'écran avant validation et doit pouvoir être modifié avant validation.

La validation rend définitif le vote et interdit toute modification ou suppression du suffrage exprimé.

Toutes les candidatures validées par l'organisateur du scrutin sont proposées aux électeurs.

Le vote blanc est également proposé au même niveau que les candidatures.

La validation du vote rend le vote définitif. Aucune modification ou suppression du suffrage exprimé n'est possible.

Alinéa 3 de l'article 13 : Le suffrage exprimé est anonyme et chiffré par le système et transmis au fichier « contenu de l'urne électronique » mentionné au II de l'article 4 où il est ainsi conservé jusqu'au dépouillement.

L'émargement fait l'objet d'un horodatage.

Comme demandé par l'alinéa, le bulletin est chiffré avec un algorithme réputé fort, RSA 3072 bits, et stocké dans l'urne sans jamais avoir été déchiffré.

La liaison entre le terminal de vote de l'électeur et le serveur des votes est chiffrée avec le protocole TLS 1.2 ou le protocole TLS 1.3, selon le terminal utilisé. C'est un chiffrement distinct de celui utilisé pour chiffrer les bulletins de vote.

L'émargement de l'électeur est horodaté avec la date du serveur de vote. Cette date est synchronisée sur un serveur de temps atomique.

Alinéa 4 de l'article 13 : La transmission du vote et l'émargement font l'objet d'un accusé de réception que l'électeur a la possibilité de conserver.

Un code faisant office d'accusé de réception est transmis aux électeurs qui ont la possibilité de le conserver ou de le retrouver dans leur espace de vote.

6.11 Article 14

Alinéa 1 de l'article 14 : Dès la clôture du scrutin, le contenu de l'urne, les listes d'émargement et les états courants gérés par les serveurs sont figés, horodatés et scellés automatiquement sur l'ensemble des serveurs, dans des conditions garantissant la conservation des données.

La présence du président du bureau de vote ou son représentant et d'au moins deux délégués de liste parmi les détenteurs de clés est indispensable pour autoriser le dépouillement.

Le dépouillement ne peut commencer qu'après l'accomplissement des formalités requises, le cas échéant, par l'article 15.

Le système de vote est scellé dès la clôture du système de vote. Les données du système de vote sont immédiatement placés au coffre-fort électronique géré par l'Ofsad.

Le système n'autorise le dépouillement qu'en présence du président du bureau de vote centralisateur ou de son représentant et d'au moins deux délégués de liste.

L'état de scellement du système est visible par les membres du bureau de vote centralisateur et les membres des bureaux de vote avant le dépouillement.

Alinéa 2 de l'article 14 : Le décompte des voix obtenues par chaque candidat ou liste de candidats apparaît lisiblement à l'écran et fait l'objet d'une édition sécurisée afin d'être porté au procès-verbal.

Le bureau de vote contrôle que la somme des suffrages exprimés et des votes blancs émis par voie électronique correspond au nombre de votants de la liste d'émargements électronique.

Lorsque tous les bulletins sont déchiffrés, le décompte des voix obtenues par chaque liste candidate est affiché clairement à l'écran.

Cet affichage comprend également le nombre de vote blancs.

Alinéa 3 de l'article 14 : Le système de vote électronique est scellé après la décision de clôture du dépouillement prise par le président du bureau de vote.

Le scellement interdit toute reprise ou modification des résultats. Toutefois, la procédure de décompte des votes enregistrés doit pouvoir être déroulée de nouveau si nécessaire.

A l'issue du dépouillement, le système de vote bénéficie d'un nouveau scellement et son contenu est placé dans le coffre-fort électronique.

Le contenu du coffre-fort électronique permet la réalisation d'une opération de recomptage si nécessaire.

6.12 Article 16

Article 16 : L'administration conserve sous scellés, pendant un délai de deux ans et dans les conditions fixées aux articles L.212-2 et L.212-3 du code du patrimoine et au 5° de l'article 6 de la loi du 6 janvier 1978 susvisée, les fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde. La procédure de décompte des votes doit, si nécessaire, pouvoir être exécutée de nouveau.

Au terme de ce délai de deux ans, sauf lorsqu'une action contentieuse a été engagée, l'administration procède à la destruction des fichiers supports. Seuls sont conservés les listes de candidats avec déclarations de candidatures et professions de foi, les procès-verbaux de l'élection ainsi que les actes de nomination des membres des bureaux de vote.

Le contenu des systèmes de vote est placé dans le coffre-fort électronique à l'issue des étapes clés des opérations de vote :

- le scellement ;
- la clôture ;
- le dépouillement.

Ces données sont conservées par NEOVOTE sous scellés pendant 2 ans.

Annexe 1 : Signature des serveurs

La version du système de vote NEOVOTE applicable pour ces scrutins est celle du 06/09/2021.

Empreinte globale du code source du système de vote	
SHA256	d332673aa38574a4eb0109e713ba17d95e9473efef40ea78340a1363ec6d8423

Empreinte du serveur	
CRC	3507GR49
SHA256	b898cb91f3ba52653eb999cc7c88a89bb25eaa2c1921febc08a01dc88294f962

Annexe 2 : Attestation d'indépendance

ATTESTATION SUR L'HONNEUR

Je soussigné	**Sébastien Roman**
agissant en qualité de	**Président**
de l'entreprise	**ITekia**

atteste sur l'honneur que les personnes d'ITekia ayant participé à la réalisation de ce rapport d'expertise indépendante :

- sont informaticiens spécialisés dans la sécurité ;

- n'ont pas d'intérêt dans la société NEOVOTE qui a créé la solution de vote à expertiser, ni dans l'Université de Nantes qui a décidé d'utiliser la solution de vote ;

- possèdent si possible une expérience dans l'analyse des systèmes de vote, en ayant expertisé les systèmes de vote par correspondance électronique, notamment via Internet, d'au moins deux prestataires différents.

Fait à Charols,

le 18/11/2021.

Annexe 3 : Glossaire

AIPD : Analyse d'Impact relatives à la Protection des Données

ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information

API : *Application Programming Interface* – Interface de programmation applicative

CNIL : Commission Nationale de l'Informatique et des Libertés

PRA : Plan de Reprise d'Activité

OFSAD : Office Français pour la Sécurité et l'Archivage des Documents

OWASP : *Open Web Application Security Project*

RGAA : Référentiel Général d'Amélioration de l'Accessibilité

RGPD : Règlement Général sur la Protection des Données

RGS : Référentiel Général de Sécurité

TLS : *Transport Layer Security*