Analyse de systèmes de vote électronique

Firmin de Barros, Thomas Gergouil, Rémy Grelard, Samuel Thibault

Master 2 CSI - Projet
Département d'Informatique, Université de Bordeaux

Analyse de systèmes de vote électronique

Firmin DE BARROS
Thomas GERGOUIL
Rémy GRELARD

supervisé par Samuel THIBAULT

Février 2022

Résumé exécutif

La sécurité des scrutins électoraux doit être assurée du fait de leur place centrale dans notre société démocratique. De plus, nous utilisons de plus en plus la technologie et internet dans des domaines sensibles comme la banque. Cela semble donc être une suite logique que de faire de même pour le vote. C'est le choix qui a été fait par l'Université de Bordeaux pour l'élection de cette année. On peut néanmoins se poser des questions sur l'accessibilité et la sécurité notamment lorsque ces nouveaux systèmes de votes sont totalement opaques sur leurs fonctionnements.

Comme le signale la CNIL, le vote électronique n'est pas encore une solution adaptée à des votes avec enjeu ou avec un grand électorat. Il n'est de plus pas fiable d'utiliser ce genre de système lorsque ni l'électorat ni les organisateurs ne connaissent son fonctionnement. Les votants ne peuvent pas lui faire confiance. Enfin, le principe de base d'un vote est de ne pas accorder sa confiance à l'organisateur du vote mais aux assesseurs choisis par les différents camps. Le rôle de ces assesseurs est réellement central et consiste à vérifier qu'aucun problème ne survienne.

L'analyse de deux systèmes de vote différents, Neovote et Belenios, nous a montré que même si techniquement ils semblent sûrs, des attaques restent envisageables dans les deux cas. De plus, une attaque contre un système de vote en ligne peut rapidement compromettre l'ensemble de l'élection tout en passant complètement inaperçue, et étant donc difficilement contestable.

Table des matières

Introduction

Cette année, les élections du conseil administratif de l'Université de Bordeaux se sont faites pour la première fois par vote en ligne avec les services fournis par un prestataire tiers : Neovote. Les principaux arguments avancés par l'arrêté fixant les modalités d'organisation de ce vote sont la flexibilité, la sécurité et la réduction des opérations de dépouillement ainsi que le développement durable. Les objectifs principaux d'un vote électronique sont aussi l'augmentation de la participation ou encore la rapidité pour obtenir les résultats.

Peut-on remplacer le système de vote traditionnel qui, de par sa simplicité et sa transparence, est bien mieux compris par la population et qui implémente des dispositifs clairs afin de garantir au mieux le bon déroulement d'un scrutin ? Alors qu'à l'opposé, les systèmes de votes électroniques sont complexes et contestés comme nous avons pu le voir durant ces élections de décembre, lors de laquelle le LaBRI a émis une motion afin d'alerter sur les nombreux problèmes de garanties des "principes fondamentaux qui commandent les opérations électorales".[12]

Le vote est un acte qui peut être critique notamment suivant l'importance de l'élection, ainsi nous présenterons tout d'abord les principes fondamentaux qui caractérisent un vote. Nous verrons ensuite les principes de sécurité mis en place par différentes solutions de vote électronique ou papier. Nous appellerons ici le vote électronique comme étant le vote électronique par internet puisque nous ne traiterons pas les solutions de vote utilisant par exemple les machines à voter. Nous essaierons ainsi de comprendre comment ces différentes solutions répondent aux enjeux imposés par un scrutin en suivant les trois étapes clés du vote : sa mise en place, le vote et sa vérification et enfin le dépouillement. Pour les solutions de vote électronique, nous avons d'un côté, Neovote et son système fermé et de l'autre, Belenios et sa solution open source. Enfin, nous approfondirons les problématiques liées à la solution de vote électronique.

1 Problématiques des systèmes de vote

1.1 Critères essentiels

Pour qu'un système de vote soit démocratique, quelques propriétés doivent être maintenues pour garantir la sécurité du scrutin et des électeurs mais aussi afin d'obtenir leur confiance envers le système de vote ce qui permettra de s'assurer de la légitimité des résultats.

Droit de vote et unicité

Seules les personnes autorisées doivent pouvoir voter, cette autorisation peut être définie par l'âge, l'appartenance à un groupe ou encore une sélection d'individus, et cette autorisation doit être à jour au moment du vote et la correspondance entre le votant physique et l'identité doit être vérifiée. Ces personnes-là ne doivent pouvoir voter que le nombre de fois autorisées.

Anonymat

Le vote est un outil démocratique important et il est utilisé pour exprimer notre opinion parfois politique ou en matière de gestion d'un organisme. On n'est en droit de ne pas révéler le contenu de son bulletin, ainsi on ne doit pas pouvoir faire de lien entre un vote et un votant.

Ce critère est difficile à maintenir si le nombre d'électeurs est petit, par exemple le vote peut être unanime ou bien un groupe de votants pourrait partager le contenu de leur vote entre eux et ainsi avoir une idée du contenu des autres votes. Ainsi l'anonymat est plus facile à garantir si le nombre de votants est grand et que la proportion de votants malhonnêtes est petite.

Résistance à la coercition

La coercition est l'action de contraindre. Dans le cadre d'un vote, il s'agît des achats (ou contraintes) de votes et le système se doit de garantir la liberté du vote. Cette problématique est liée à l'anonymat et à la vérification de son vote. En effet, une personne qui achèterait un vote ou qui contraindrait un électeur peut souvent vérifier que le vote a bien été effectué mais le système est tout de même résistant si le votant peut s'isoler et qu'une preuve de vote ne divulgue pas son contenu.

Vérification de son vote

Il faut pouvoir s'assurer que son vote soit bien comptabilisé lors du dépouillement et que le contenu du vote n'a pas été changé entre le moment du vote et celui de la comptabilisation.

Transparence et confiance

Une élection pourrait être rendue nulle si la confiance d'une grande partie de l'électorat envers l'organisation du scrutin est perdue. Ainsi ce critère renvoie à la possibilité de tout un chacun de pouvoir comprendre les mécanismes à l'œuvre mais aussi de pouvoir attester du respect du protocole tout au long de l'élection. Lors d'élections trop importantes pour qu'un simple électeur puisse s'assurer de ce dernier point, cette confiance peut être accordée à plusieurs tiers, généralement aux assesseurs. Nous définirons leurs rôles plus en détails dans les parties d'analyse des systèmes.

1.2 Recommandations de la CNIL sur le vote électronique

La délibération n°2019-053 du 25 avril 2019 de la CNIL [4] (Commission Nationale de l'Informatique et des Libertés) présente ses nouvelles observations quant aux systèmes de votes électroniques et régit encore aujourd'hui ce type de vote en France. En effet, depuis le 25 mai 2018 le Règlement Général sur la Protection des Données (RGPD) est entré en application en Europe et les systèmes de vote en ligne n'ont plus à être déclarés à la CNIL. Ce qui rend difficile leur contrôle et réduit la confiance vis-à-vis de leur fiabilité.

Sans pour autant interdire les votes électroniques via internet, la CNIL établit ici des objectifs de sécurité à atteindre en fonction de l'importance du scrutin.

La commission établit donc cette importance par le biais de trois niveaux de risque à l'aide de plusieurs critères comme la motivation et les ressources des menaces, les potentiels conflits d'intérêts avec les administrateurs, le nombre de votants et les enjeux de l'élection. Ces trois niveaux peuvent être attribués à l'aide d'une grille de 10 questions fermées fournie par la CNIL et des exemples d'applications sont donnés :

- Niveau 1 - Non important : l'élection d'un représentant de classe.
- Niveau 2 - Risque modéré : élections de représentants du personnel au sein d'organismes ou encore au sein d'un ordre professionnel.
- Niveau 3 - Risque important : élections de représentants du personnel au sein d'organisations importantes, à grande échelle et dans un cadre conflictuel.

Il est dit dans cette délibération que pour tout système de vote électronique via internet de niveau 2 et 3, il est nécessaire pour les organisateurs de mandater un expert indépendant afin de notamment évaluer le choix du niveau choisi pour l'élection. Cette expertise se doit aussi de couvrir l'ensemble du système avant le scrutin (logiciel, serveur...).

Notons donc que la CNIL émet, dans ce même document, des réserves quant à l'utilisation de la solution du vote électronique d'autant plus via internet pour des votes politiques.

2 Fonctionnement des systèmes de vote pour les votants

2.1 Neovote

Nous analyserons le système de Neovote en fonction du scrutin survenu en décembre dernier à l'Université de Bordeaux.

2.1.1 Vote

Les votants reçoivent un mail indiquant les modalités du vote, dans notre cas exclusivement par voie électronique, la période du vote, ainsi que les informations nécessaires pour voter : le lien du vote, un identifiant et la nécessité d'avoir son code personnel ou son numéro INE. Une fois l'identifiant et le numéro INE saisis sur le site, on obtient un mot de passe qui sert à valider le vote. On peut ensuite voter.

2.1.2 Vérification

Après avoir voté, le site donne une preuve de vote. Il est possible d'aller sur le site de vérification du vote après le dépouillement et renseigner le serveur de vote, notre mot de passe et la preuve de vote afin de vérifier qu'il est bien dans l'urne. Si c'est le cas, le site signale que le bulletin est bien dans l'urne et affiche les résultats.

2.2 Belenios

2.2.1 Vote

Les votants reçoivent un mail contenant le lien du vote et un code de vote. Pour voter, il faut se rendre sur le site grâce au lien puis indiquer son code de vote. On peut ensuite voter. On doit valider notre vote et pour cela il y a plusieurs moyens au choix de l'organisateur : avec un mot de passe envoyé par mail ou en s'identifiant sur un CAS (Central Authentication Service). Si la validation est approuvée, le vote est comptabilisé.

2.2.2 Vérification

Lors du vote on nous donne un numéro de suivi, on peut vérifier que ce numéro de suivi se trouve dans la liste des bulletins qui est disponible après avoir voté. Cette liste est consultable jusqu'à la suppression du vote.

2.3 Vote traditionnel

2.3.1 Vote

On considérera uniquement le cas où le vote a une importance suffisante pour justifier la mise en place d'un mode de scrutin strict. C'est le cas par exemple pour les élections présidentielles. On met alors en place un vote avec des urnes transparentes, des isoloirs, des bulletins en papier et des enveloppes, toutes identiques. On appellera ce système : le système de vote traditionnel. Pour voter, un individu doit remplir certains critères selon l'élection (adhérer à un parti, avoir plus de 18 ans, etc.).

Le jour de l'élection, il doit se rendre sur le lieu de vote. Sur place, il prouve qu'il est bien un votant légitime (présence sur la liste, possession d'une carte d'adhérent à jour, ...). Il remplit son bulletin de vote de manière anonyme (présence d'un isoloir). Il va ensuite placer son vote dans l'urne. S'il y en a une, le votant doit signer la feuille d'émargement.

2.3.2 Vérification

Une fois que le votant a placé son bulletin dans l'urne, celui-ci est mélangé aux autres bulletins. Comme les bulletins sont tous identiques de l'extérieur, il n'est pas possible de vérifier à tout moment si le nôtre est dans l'urne. Un bulletin qui se distingue est considéré comme invalide et devient nul. Cependant, il est possible de rester tout le long du vote pour vérifier qu'aucune manipulation n'est faite sur l'urne ou sur les bulletins. C'est le rôle des assesseurs de surveiller le vote du début à la fin mais il est aussi possible pour un électeur de vérifier le bon déroulement du vote jusqu'au dépouillement.

3 Mise en place du système de vote

3.1 Neovote

3.1.1 Information de connexion

Dans le cadre d'un vote électronique, il est nécessaire de donner les informations de connexion aux futurs votants. Dans le cas du vote à l'Université de Bordeaux, ces informations nous ont été transmises via un mail "personnel et confidentiel". Ce mail indique tout d'abord le serveur de vote (`https://vote595.neovote.com`) ainsi qu'un identifiant de vote. Il faut aussi son numéro INE pour les étudiants ou le code personnel pour le personnel de l'université. C'est une fois connecté que l'on peut obtenir le mot de passe qui servira à valider le vote. Pour ce faire, on choisit une adresse mail ou un numéro de téléphone et le mot de passe seront envoyés respectivement par mail ou bien par SMS.

3.1.2 Analyse de l'en-tête du mail

Chiffrement

Tout d'abord, le mail est envoyé depuis le serveur de mail de Neovote sur celui de l'Université à l'aide du protocole ESMTPS (Extended Simple Mail Transfer Protocol). C'est une version sécurisée du protocole ESMTP qui ajoute l'extension STARTTLS. Cela consiste à ce que le client qui se connecte essaie d'initier une connexion TLS avec le serveur. C'est un chiffrement opportuniste c'est-à-dire que si la négociation ne se passe pas bien, alors la communication n'est pas chiffrée. Le fait que l'on voit dans l'en-tête qu'ESMTPS a été utilisé indique que cette négociation a réussi.

Ce chiffrement doit empêcher un attaquant qui se trouverait sur le chemin entre les deux serveurs (Man in The Middle) de pouvoir récupérer les informations que contient le mail. Cependant, un attaquant réussissant à s'interposer entre les serveurs de Neovote et de l'Université peut volontairement faire échouer la négociation et bloquer le chiffrement TLS. La communication sera donc en clair et il pourra récupérer le mot de passe. Il faut donc que le serveur de Neovote s'assure que le mail envoyé soit chiffré avec un niveau de chiffrement fort.

Signature

Ce mail comporte aussi une signature DKIM (DomainKeys Identified Mail) afin de vérifier la provenance de celui-ci.

Pour la vérifier, on récupère la clé publique associée à la clé privée qui a été utilisée grâce à une requête DNS. Il est ensuite possible de vérifier cette signature et ainsi le fait que le mail provienne bien des serveurs de Neovote.

La signature permet d'éviter le phishing de la part d'un attaquant qui essaierait de se faire passer pour Neovote. Cependant, il faut que le logiciel de mail des votants s'assure qu'il possède bien une signature et que celle-ci est valide. Or ce n'est généralement pas le cas.

Transfert du mail

Après avoir été transféré sur les serveurs de mails de l'université, le mail est transféré entre deux serveurs 'mta-in02.u-bordeaux.fr' et 'v-zimboxe03.srv.u-bordeaux.fr' en utilisant ESMTPS.

3.1.3 Récupération de mot de passe

Il existe une procédure en cas de perte du mot de passe ou de l'identifiant. Dans ce cas, il faut se connecter au site `https://vote595.neovote.com` avec son numéro INE ou son code personnel. Cette page demande certaines informations ainsi qu'un numéro de téléphone afin de saisir le contenu d'un SMS envoyé comme présenté dans la Figure 1.

FIGURE 1 – https ://vote595.neovote.com/support

Dans ce formulaire, aucune des informations demandées n'est réellement secrète. En effet, si un attaquant cible un votant en particulier, alors il possède son prénom et son nom de famille qui sont des informations publiques. La date de naissance est très souvent facilement accessible (via les réseaux sociaux par exemple). Le numéro matricule dans le cas d'un personnel de l'Université de Bordeaux n'est pas non plus un secret puisqu'il est lisible sur sa carte Aquipass. Pour un étudiant, le numéro INE n'est pas visible sur sa carte étudiant mais sur certains documents officiels comme les relevés de notes du Baccalauréat ou de l'enseignement supérieur ou sur un certificat de scolarité. Ces documents n'étant pas destinés à être gardés secrets, il est raisonnable de penser qu'un tiers puisse avoir accès à cette information.

Se faire passer pour quelqu'un d'autre afin de récupérer son mot de passe ne semble pas impensable. Ceci peut engendrer une faille si un attaquant peut détourner le mail envoyé par le serveur de Neovote à celui de l'Université de Bordeaux, il pourrait choisir de renvoyer ce mail au moment où son attaque est en place.

3.2 Belenios

3.2.1 La création du vote par l'organisateur

L'organisateur possède plusieurs choix lors de la création du vote, il peut donc adapter ses choix en fonction de l'importance de l'élection et de la sécurité nécessaire. Tout d'abord, le code source étant disponible, il est laissé à l'organisateur du vote le choix d'utiliser le serveur de Belenios ou un serveur tiers avec l'aide du code source. Les deux solutions ont leurs avantages et leurs inconvénients. Utiliser le serveur de Belenios est plus simple mais l'élection dépend d'un serveur sur lequel l'organisateur n'a aucun contrôle. Utiliser un serveur tiers est plus compliqué mais on est indépendant, les données telles que les adresses mails des votants ne sont pas envoyées sur un serveur externe sur lequel nous n'avons pas le contrôle sur la sécurité et de l'utilisation des données.

Pour des questions pratiques et de confiance vis-à-vis des électeurs, l'organisateur du vote peut déléguer l'hébergement à un tiers dont on peut évaluer l'indépendance. On peut en effet vouloir que l'organisateur n'héberge pas lui-même le vote.

L'organisateur a ensuite le choix pour la génération des codes de vote et pour le moyen de validation.

3.2.2 Codes de vote

L'organisateur d'une élection a deux options : ou bien les codes de vote sont générés et envoyés par le serveur, ou bien vous devez désigner une autorité de codes de vote qui se charge de cette tâche.

Générer les codes de vote sur la plateforme est la solution la plus simple. Le serveur génère les codes de vote (privés), les envoie par mail aux votants et stocke uniquement la partie publique correspondante. L'organisateur a accès à l'ensemble des codes de vote, il lui est conseillé d'en conserver une copie dans le cas où un électeur perd le sien. Ces codes doivent être détruits dès que l'élection est terminée. Cette solution est celle qui offre le moins de sécurité. En effet, si le serveur du vote est compromis avant l'élection, l'attaquant aura alors accès aux codes censés être privés et pourra ajouter des bulletins dans l'urne et modifier le résultat de l'élection.

Utiliser une autorité de génération de codes de vote est la solution la plus sécurisée. Une URL est transmise à l'organisateur de l'élection qu'il doit à son tour transmettre à l'autorité de génération des codes de vote. L'autorité pourra ainsi générer sur son propre ordinateur les codes de vote privés qu'il devra transmettre aux votants et la partie publique qu'il devra envoyer au serveur. Cela suppose que l'autorité de génération ait des compétences en informatique pour écrire et/ou utiliser un script lui permettant de transmettre les codes à l'électorat si le nombre de votants est important. En plus, cette option permet de sécuriser les mails contenant les codes de vote de la manière que l'on souhaite.

3.2.3 Moyen de validation

L'organisateur d'une élection a trois options : il peut choisir d'envoyer le mot de passe de validation dans un mail à la création du vote, il peut aussi décider qu'un mail soit envoyé pendant le vote et enfin il peut utiliser un service d'authentification externe.

Envoyer le mot de passe de validation dans un mail à la création du vote peut être utile en cas d'élections multiples, cela évite de générer un mot de passe par élection. C'est la solution la moins sûre, une attaque par force brute peut être envisagée pour trouver une combinaison code de vote

et mot de passe bien que très peu probable voire impossible au vu du nombre de combinaisons possibles. Cependant, si un attaquant a accès à la boîte mail d'un votant, il possède le code de vote et le mot de passe qui sont tous deux envoyés à la création du vote.

Envoyer le mot de passe pendant le vote est plus sécurisé, on doit renseigner l'adresse sur laquelle on a reçu la preuve de vote puis on reçoit un mot de passe unique pour chaque tentative de vote. L'attaque par force brute est rendue impossible car il est nécessaire d'avoir la combinaison code de vote, adresse email et mot de passe. Si l'attaquant a accès à l'adresse email d'un votant, il lui est possible de voter.

Pour la troisième option, après avoir voté, on est redirigé vers la page de connexion CAS indiquée par l'organisateur de l'élection. C'est le choix le plus sécurisé, l'attaquant à besoin de plus qu'un accès à la boîte mail du votant, il a aussi besoin de l'identifiant et du mot de passe du service d'authentification.

3.2.4 Autorités de déchiffrement

Par défaut aucune autorité n'est choisie, il n'y a qu'une seule clé de déchiffrement qui est stockée sur le serveur, ce choix est déconseillé par Belenios sauf dans le cas d'une élection test. L'organisateur peut donc choisir des autorités de déchiffrement en plus du serveur : chaque autorité possède une clé de déchiffrement. Il s'agit alors d'un système de chiffrement à seuil, si le serveur et suffisamment d'autorités extérieures veulent déchiffrer alors le vote est dépouillé sinon on ne peut pas connaître les résultats du vote.

3.2.5 Mail et analyse de l'en-tête

Lorsque l'élection est créée, les votants reçoivent un mail avec les informations nécessaires pour voter comme le site du vote, le code de vote ou le mot de passe.

Le mail de Belenios possède un en-tête similaire à celui de Neovote. On peut y voir que le mail est transmis depuis le serveur de Belenios à l'aide du protocole ESMTPS sur les serveurs de mail de l'Université de Bordeaux (si on choisit une adresse mail de l'université). Il possède également une signature DKIM.

Nous pouvons donc tirer la même conclusion que pour Neovote quant à l'utilisation du protocole ESMTPS. Et cela renforce la nécessité de faire appel à une autorité de codes qui se chargera d'envoyer les codes de vote, et pour lesquels l'organisateur du vote peut demander d'utiliser un protocole qui s'assure de l'utilisation d'un chiffrement fort.

3.3 Vote traditionnel

Pour mettre en place un système de vote traditionnel, les moyens financiers, humains et matériels croissent en fonction du nombre de votants. Si le nombre de votants est trop important, il faut aussi répartir les votants de manière plus ou moins homogène dans les lieux de votes : le nombre de personnels (assesseurs, scrutateurs...) et de matériels (urnes, isoloirs...) est multiplié. De plus dans le cas d'une grande élection, il faut aussi arranger un moyen de voter pour les résidents à l'étranger.

Il faut aussi envoyer les cartes électorales, d'adhésions... Et imprimer les bulletins, qui doivent être d'un nombre égal pour chaque candidat. Ainsi la question écologique se pose elle aussi mais ce rapport n'essaiera pas de répondre à cela.

3.4 Liste des votants

L'établissement de la liste des votants est un point essentiel et l'un des points critiques majeurs. Il faut s'assurer que toutes les personnes possédant le droit de vote pour cette élection et uniquement ces personnes soient sur cette liste. Il faut de plus s'assurer que dans le cas où l'élection est assez grande pour avoir besoin de plusieurs lieux de votes et donc de plusieurs de ces listes, une personne n'est pas inscrite sur plusieurs listes.

La liste de votant est souvent à l'origine de fraude (ou de fraude potentielle), en effet, il est courant que le nom d'une personne ne soit pas retiré des listes de votants lors d'un déménagement. On se retrouve alors avec des personnes pouvant voter dans plusieurs bureaux de vote. Il y a aussi des cas de personnes décédées toujours présentes sur les listes de votants.

Ce problème n'est pas réglé mais peut être diminué par le vote électronique qui permet de définir des moyens de vérifier l'identité grâce à des services spécialisés, par exemple un CAS (Central Authentication Service). Il n'existe plus qu'une seule et même liste de votants.

Ceci est évidemment sous couvert que ces services soient fiables dans la mise à jour de leurs informations et dans la recherche d'informations incohérentes (plusieurs comptes pour la même identité...). Mais il faut aussi qu'ils respectent le RGPD.

Le vote traditionnel pourrait aussi adopter ce genre de mécanismes pour aider à créer les listes de votant cependant ce n'est pas le cas.

4 Vote et vérification de votes

4.1 Neovote

4.1.1 Certificat du site de vote

Le vote étant effectué sur internet, l'utilisateur doit pouvoir s'assurer de l'authenticité du serveur et de la confidentialité et de l'intégrité de l'échange. Pour ce faire il est logique de penser au protocole HTTPS.

Ce protocole utilise les certificats SSL pour fonctionner. Ils sont délivrés par des autorités de certifications (ou CA) et leur fiabilité peut être évaluée par rapport à plusieurs critères.

Le vote ayant été effectué sur le site : 'https ://vote595.neovote.com/', nous pouvons analyser le certificat utilisé. Il est délivré par GlobalSign qui est une entreprise reconnue dans la délivrance de certificats.

Vérification de la propriété

Il est ainsi signé par 'GlobalSign RSA OV SSL CA 2018'. On peut y voir la notation 'OV' qui signifie 'Organization Validated'. Pour la distribution de ce type de certificat, il doit y avoir une vérification de la possession du droit exclusif de l'organisation en question sur le nom de domaine. Ce sont des vérifications supplémentaires par rapport aux certificats DV (Domain Validated) mais inférieures aux vérifications faites pour les certificats EV (Extended Valitation). Avec ce type de certificat, le nom de l'entreprise est ajouté au certificat :

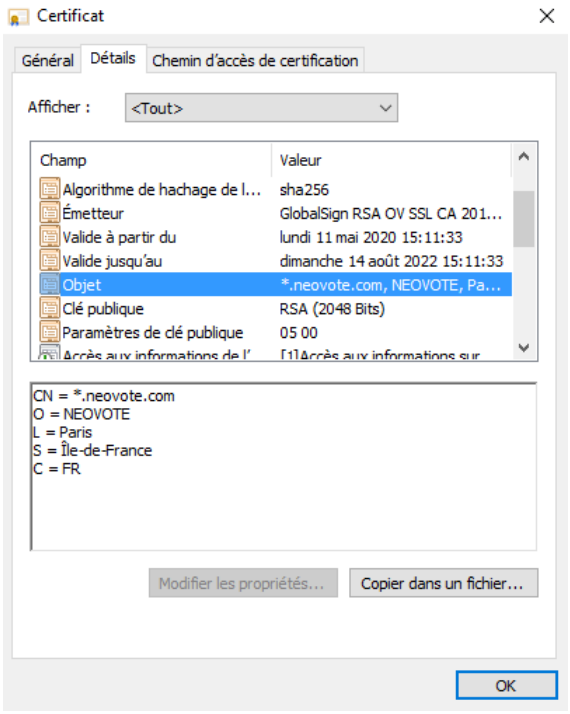

FIGURE 2 – Certificat de vote595.neovote.com

Comme mentionné précédemment, il existe un niveau de sécurité supplémentaire pour les cer-

tificats : les certificats Extended Validated ou EV. Ils sont utilisés pour les applications sensibles (banque, e-commerce...) et pourraient donc être nécessaire pour une application de vote.

Pour délivrer ce type de certificats des étapes de vérifications plus complètes sont ajoutées et permettent de s'assurer de l'identité du propriétaire. Il y a donc des vérifications :

- de l'existence légale, physique et opérationnelle de l'organisation
- des informations rajoutées par rapport aux registres légaux
- du droit exclusif de l'utilisation du nom de domaine spécifié
- de l'accord de l'organisation pour l'émission du certificat

Par exemple on peut voir sur le certificat de ssl.com :

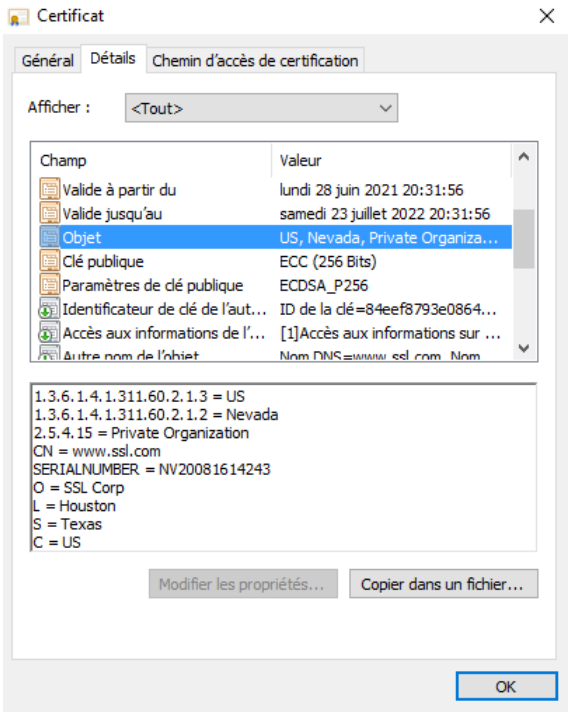

FIGURE 3 – Certificat EV de ssl.com

Wildcard Certificat

Ce certificat est plus précisément délivré pour le domaine '*.neovote.com'. Il s'agit d'un wildcard certificat, c'est-à-dire que ce certificat peut être utilisé par tous les sous-domaines de neovote.com. Ce type de certificat est utilisé afin de faciliter la gestion et de réduire les coûts des certificats : un seul certificat est nécessaire pour tous les sous-domaines.

La solution de Neovote consiste à organiser les votes sur des serveurs différents, il est donc nécessaire pour eux de posséder de nombreux serveurs. Pour faciliter la gestion et réduire les coûts, ils utilisent donc un "wildcard certificat". Ces certificats ne sont pas disponibles avec la sécurité EV puisqu'il faudrait lister tous les sous-domaines dans le certificat ce qui peut ne pas être voulu.

Il existe cependant une option multi-domain proposée par GlobalSign.

Sécurité liée à la validité

Une durée de validité courte assure un renouvellement des clés privées régulier. Cela permet aussi une propagation des mises à jour de sécurité plus rapide, en effet, il n'y a pas besoin d'attendre trop longtemps que tous les certificats soient révoqués pour changer un algorithme. De plus, cela permet une vérification des identités plus régulière, ce qui les rend plus fiables. Enfin, les certificats révoqués avant leur fin de validité seront plus rapidement repérés si la liste des certificats révoqués n'est pas vérifiée.

La durée de validité d'un certificat chez GlobalSign est de 397 jours (13 mois) comme indiqué par le CA/B (Certification Authority Browser Forum) le consortium sur des autorités de certification, browser...

Sécurité des algorithmes utilisés

L'algorithme de signature est sha256RSA et la clé publique RSA est de 2048 bits. Ce qui suit les recommandations du CA/B forum et de la NIST (National Institute of Standards and Technology).

4.1.2 Certificat du site de vérification

Le certificat utilisé par le site de vérification est quant à lui délivrer par Let's Encrypt.[9]

Let's Encrypt est la plus grosse autorité de certification du monde en nombre de sites certifiés. Cependant, la raison est financière plutôt que la preuve d'une grande confiance en la sécurité de leur solution. En effet, les certifications sont gratuites et automatiques et donc plus rapides à obtenir.

Ce procédé d'auto-signature est largement questionné et est principalement utilisé pour des sites qui ne nécessitent pas le transfert de données sensibles (numéro de carte bancaire,...). Cependant, le site de vérification demande justement des données que l'on peut considérer comme sensibles, en effet, le mot de passe du vote et la preuve de vote sont supposés rester secrets.

De plus, il s'agit ici d'un certificat DV. En effet, Let's Encrypt ne pouvant pas automatiser les vérifications, ils ne peuvent pas délivrer de certificats OV et EV. Ce type de service propose donc moins de vérifications quant à l'identité des propriétaires d'un site censé recevoir des informations secrètes (mot de passe et preuve de vote). Le même niveau de sécurité que le site du vote est tout de même utilisé pour l'algorithme de signature et pour la clé.

4.1.3 Vote

Nous avons assez peu de détails sur la partie technique de la solution proposée par Neovote. En effet, leur système est sous secret défense, il nous reste donc les quelques informations présentes sur leur site internet [10] :

- Des serveurs HSM de niveau EAL5+ : cela permet de générer et stocker des clés cryptographiques. Le niveau EAL5+ signifie que le produit a été testé sur sa sécurité.[18][16]

- De nombreux tests et homologations sont réalisés par des acteurs différents : ministère de l'intérieur, bureaux de vote, parties prenantes
- Les composants sont intégralement développés par eux (Cœur cryptographique, protocoles communicatifs...).

Neovote développe ses propres composants mais le niveau de sécurité est discutable puisque cela va à l'encontre du principe de Schneier [3]. En effet, étant donné que le système n'est pas ouvert, puisqu'il est sous secret défense, il ne peut pas être vérifié par les pairs. Personne ne peut donc s'assurer que tous les composants sont suffisamment robustes.

On peut aussi y lire "Solution homologuée par le Conseil d'État, le Sénat, l'Assemblée nationale, le Ministère de l'Intérieur et la DGSI". Cela n'a pas vraiment de sens puisque ce ne sont pas des organismes d'homologation et notre demande pour les documents d'homologation est restée sans suite.

4.1.4 Code source de vérification

Le code source de la vérification de la preuve de vote était téléchargeable sur le site de vérification `https://verifier-mon-vote.fr/`. Cela est nécessaire afin de respecter le niveau CNIL-3 car la solution de vote doit "Permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers"[4]. Ce code source n'est plus accessible en ligne et le vote ne respecte donc plus cet objectif pour avoir le niveau de sécurité CNIL-3.

La preuve de vote obtenue est d'abord décodée depuis le format base64 avant d'être déchiffrée par AES. Le serveur procède ensuite à une vérification de la cohérence du déchiffrement en validant un CRC32. On obtient donc le hash de notre vote. Après cela, il recherche dans la liste de tous les bulletins la présence de notre hash.

Nous avons pu écrire nous-même un script pour obtenir notre hash puisque leur solution répondait à ce moment-là au niveau d'exigence CNIL-3. En effet, la clé de chiffrement AES était présente, ce chiffrement donne donc seulement une impression de sécurité puisque tout le monde pouvait accéder à la clé et qu'AES est un chiffrement symétrique.

Avec notre hash, nous sommes aussi censés retrouver un sel au début des données. Ce sel est commun à tout le monde et visible dans le code source. Ceci réduit son utilité.

Après la vérification de la preuve de vote, le serveur refait un comptage du scrutin. Celui-ci est fait indépendamment de celui qui donne les résultats officiels et peut-être demandé par tous les votants.

La documentation de Neovote n'indique pas si la preuve de vote révèle le vote qui correspond. Cette question est d'autant plus pertinente que Neovote demande à ce que chaque personne garde cette preuve secrète. Après étude du script, celui-ci semble parcourir l'ensemble des preuves de vote pour vérifier que le hash du vote chiffré correspond bien à notre preuve de vote. Cela permet de vérifier que notre preuve de vote est cohérente avec le vote. Cependant, on ne peut pas calculer le chiffrement du vote et voir s'il est cohérent avec notre vote réel. Si on le pouvait, il serait possible de fournir à un tiers une preuve de ce qu'on a voté ce qui fait que le système n'est plus résistant à la coercition. Les deux approches présentes donc des défauts majeurs.

4.2 Belenios

4.2.1 Certificat

Rappelons tout d'abord, que la solution de vote électronique proposée par Belenios peut être installée par les gérants de l'élection et ils peuvent ainsi gérer leurs propres certificats.

Si les élections sont organisées sur leur site alors les votes et leur vérification se font sur "belenios.loria.fr". La solution de Belenios, se faisant donc sur un seul et même site pour tous les votes, ne nécessite pas de Wildcard Certificat.

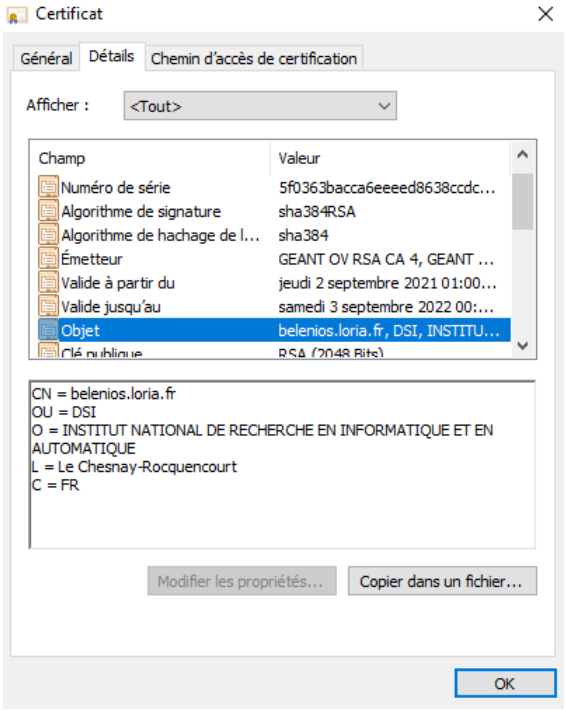

FIGURE 4 – Certificat de belenios.loria.fr

Vérification de la propriété

Le certificat est délivré par la société Sectigo, qui est elle aussi une société reconnue dans la délivrance de certificats. Tout comme le certificat du site de vote du Neovote, il s'agit d'un certificat OV et la vérification n'est pas au plus haut niveau possiblement fourni par les autorités de certifications mais cela prouve tout de même que des vérifications de bases ont été effectuées.

Autres sécurités

Le certificat a été délivré avec une période de validité d'un an, ce qui respecte les recommandations du CA/B.

L'algorithme de signature utilisé est sha384RSA avec une clé publique RSA de 2048 bits ce qui suit aussi les recommandations du CA/B et de la NIST.

4.2.2 Le protocole de vote

Le protocole de vote de Belenios est une évolution du protocole Helios. Le protocole de vote se base sur un chiffrement asymétrique, le chiffrement El Gamal. Chaque scrutin possède une clé publique propre qui permet à chaque votant de chiffrer leur vote. Les clés privées sont réparties entre les différentes autorités de déchiffrement.

4.3 Vote traditionnel

Pendant le vote, la sécurité est essentiellement physique, on peut surveiller les votes et l'urne, ils sont tangibles on peut les voir. Il y a une certaine confiance du fait que tous les éléments soient visibles.

4.3.1 Surveillance du vote

Plusieurs formes d'autorité peuvent surveiller le bon déroulement du vote :

- des assesseurs, qui sont des électeurs et qui sont désignés par différents candidats. Cela assure une sécurité, les assesseurs ne souhaitant pas la même issue pour le vote on peut leur faire confiance, il y a peu de chances qu'ils changent l'issue du vote ensemble.

- des votants peuvent surveiller l'urne. Si, par exemple lors d'une assemblée générale, l'ensemble des votants sont sur place alors une autre autorité n'est pas nécessaire.

- un tiers parti qui est là dans l'unique but de vérifier le bon déroulement du vote. L'organisateur se doit de choisir une autorité fiable et indépendante afin d'assurer la sécurité du vote.

L'autorité est chargée de s'assurer de la légitimité des votants, du recensement des votants via en général une liste d'émargement et de l'absence de fraude.

Il ne faut cependant pas tomber dans un sentiment de fausse sécurité, ce système possède des faiblesses comme le montrent les cas de fraudes électorales. Il faut aussi prendre en compte le facteur humain, des erreurs d'inattention peuvent être commises.

4.3.2 Fraudes

Les fraudes électorales et erreurs humaines peuvent se décliner de plusieurs façons [17] :

- le bourrage d'urne qui consiste à mettre plusieurs votes en même temps dans l'urne
- l'échange de vote, les votes étant tous similaires en extérieur
- la dégradation des bulletins afin de les rendre nuls
- voter pour des personnes absentes, les votants étant assignés au bureau suivant son adresse, on peut connaître un autre votant et savoir qu'il ne viendra pas voter

Le fait qu'il peut y avoir plusieurs lieux de vote et un quota maximum d'électeurs par bureau de vote permet de réduire son impact. Par exemple, si une fraude est commise dans un bureau de

vote lors d'une élection présidentielle, l'issue du scrutin ne va pas changer car le nombre de votant dans un bureau de vote est trop faible par rapport au nombre total d'électeurs.

À l'inverse, la fraude d'un vote électronique peut être arbitrairement grande. Si l'on imagine qu'un attaquant réussit à voter pour d'autres personnes alors il n'y a potentiellement rien qui l'empêche de changer le résultat du scrutin.

4.3.3 Certification

L'équivalent du certificat SSL pour une élection papier importante (présidentielle, référendum...) serait l'adresse du bureau de vote sur la carte d'électeur. De plus, il s'agit dans la plupart des cas d'établissements importants et bien connus comme une école ou une mairie. Pour une élection plus petite, on peut connaître les organisateurs ou le lieu de regroupement habituel.

5 Dépouillement

5.1 Neovote

Le dépouillement est privé, le public n'a pas accès aux détails des résultats ou à qui possède les clés de déchiffrement. Ceci fait barrage à la nécessité de transparence ce qui cause des problèmes de confiance envers ces résultats et donc en la légitimité du scrutin.

Comme vu durant le vote à l'Université de Bordeaux, le rôle des assesseurs n'est pas expliqué.[15] Les électeurs ne savent pas comment l'intégrité du scrutin a été vérifiée.

5.2 Belenios

Le dépouillement de Belenios peut se faire de deux façons, par défaut, le serveur de l'élection possède la clé de déchiffrement (déconseillé) ou bien des autorités de déchiffrement sont nommées en plus du serveur. Dans le dernier cas, un chiffrement à seuil est utilisé : il faut un certain nombre d'autorités pour que le serveur déchiffre l'urne avec les clés qu'ils ont générées localement pour que le résultat soit visible. Une seule autorité ne peut pas dépouiller l'urne, cela ressemble au vote traditionnel.

Le système de chiffrement El Gamal est un homomorphisme, à partir de deux chiffrés on peut en créer un troisième et lorsque l'on déchiffre les deux premiers ou le troisième on obtient les mêmes informations. Ainsi n'importe qui peut, sans avoir de clé, calculer le chiffrement du résultat à partir des votes chiffrés. De cette manière, seul le résultat final a besoin d'être déchiffré. L'anonymat des votants est ainsi préservé car on ne déchiffre aucun vote de manière individuelle.

Les autorités de déchiffrement produisent en plus une preuve zero-knowledge pour prouver aux votants que le scrutin a bien été déchiffré. La preuve peut être vérifiée avec l'aide d'outils tiers.

5.3 Vote traditionnel

Pour le dépouillement, l'urne scellée par plusieurs serrures est ouverte. Les votes sont décomptés en présence des assesseurs et des autres autorités s'il y en a. En général n'importe qui peut venir assister au dépouillement afin de s'assurer qu'il n'y ait pas d'erreur à cette étape. À la fin du dépouillement, on vérifie que le nombre de voix ne diffère pas du nombre de votants ayant émargé. En pratique, il arrive que le nombre de votes ne corresponde pas exactement mais on peut vérifier que la différence ne change pas l'issue du scrutin.

6 Problèmes liés à la solution électronique

6.1 Coercition

Le vote électronique sur internet est de par nature incompatible avec le critère de résistance à la coercition. En effet, le vote se fait sur un appareil personnel (ordinateur, téléphone portable...) et depuis un lieu où les organisateurs du vote n'ont pas de contrôle sur le respect de l'anonymat. Nous pouvons, de façon réaliste, penser à un possible achat de vote bien plus massif qu'avec le vote traditionnel et ce avec peu de moyens. Par exemple, si tous les votants sont forcés d'envoyer les informations nécessaires afin de voter à un groupe tiers.

6.2 Accessibilité

Les étapes du vote peuvent être complexes, d'autant plus pour une personne qui n'utilise pas d'appareils électroniques. Il peut alors y avoir besoin d'une aide extérieure. Cela enfreint potentiellement le critère d'anonymat et peut aussi rejoindre le point précédent, dans le cas d'une aide malhonnête. Cette situation n'est pas insignifiante, en France en 2019 d'après une étude de l'INSEE, l'illectronisme concernerait 16,5% de la population.[13] Pour l'élection à l'Université, des kiosques de vote avaient été mis à disposition, et de l'aide au vote a pu être fournie. Cependant des problèmes d'anonymat et de coercition demeurent.

Le critère de Transparence et de Confiance est aussi incompatible. Les solutions de votes électroniques peuvent être fermées donc tout simplement non-transparentes mais les solutions ouvertes ne le sont en réalité pas beaucoup plus du fait de leur accessibilité. Il faut pouvoir comprendre les mécanismes employés dans la mise en œuvre de la solution, et il faut donc les connaissances mathématiques et informatiques pour comprendre les notions de chiffrement, de signature, de hachage et bien d'autres. De plus, les solutions sont très volumineuses, nous pouvons estimer que dans la solution open source de Belenios, il y a des milliers de lignes de code.

À titre de comparaison, un système de vote traditionnel est simple, un enfant sachant lire, écrire et compter peut comprendre et vérifier le bon déroulement du scrutin. À l'inverse, la documentation fournie par Neovote n'explique pas aux électeurs comment avoir confiance dans le bon déroulement du scrutin.

6.3 Organisation

La complexité apportée par la solution électronique engendre des problèmes au niveau de l'organisation du vote. En effet, les organisateurs ne sont pas forcément au courant de la façon de gérer les conséquences de ce choix de faire un vote électronique.

Un exemple récent est la primaire Populaire. Le problème vient de la façon de vérifier l'identité d'un votant afin de faire en sorte qu'une personne ne puisse voter qu'une seule fois. En effet, des personnes ont pu voter plusieurs fois puisqu'il ne fallait fournir qu'une carte bancaire, une adresse mail et un numéro de téléphone. Il est assez simple d'obtenir d'autres triplets de ces informations à l'aide de cartes téléphoniques temporaires, d'adresses mail gratuites ou encore de cartes ticket restaurant qui étaient acceptées à la place d'une carte bancaire.[1][5]

6.4 Vérification

La vérification du bon déroulé du vote électronique est en partie gérée, comme pour le vote papier, par les assesseurs à qui les électeurs délèguent leur confiance. Néanmoins, les fraudes visant les systèmes électroniques peuvent être exécutées en dehors du champ de vision des assesseurs, des organisateurs et des votants. Il y a donc une plus forte nécessité qu'avec le vote papier à ce que les électeurs vérifient eux-mêmes leur vote. Ceci ajoute une limitation au vote électronique puisque l'on sait que tout le monde ne le fait pas.

De plus, il existe un conflit dû au degré de vérification : si une preuve de vote ne permet pas de vérifier son contenu, alors l'électeur ne peut pas être sûr que le serveur a bien reçu son choix. Si la preuve de vote permet de vérifier son contenu, alors il y a potentiellement un problème de coercition et d'anonymat.

Avec le vote papier, c'est le fait que l'urne ne soit pas modifiée qui assure que le contenu du vote n'a pas changé.

6.5 Expertise

Une expertise est obligatoire pour un vote électronique de niveau 2 et 3, cependant cette mesure a des limites. Une vérification de la solution est faite à un certain moment, ce qui ne garantit pas qu'il s'agit bien des mêmes logiciels au moment du vote.

Le vote électronique est une solution informatique et par conséquent il y a toujours une possibilité d'erreurs informatiques. Il y a bien sûr des problèmes d'erreurs avec le vote traditionnel, mais ce genre de problèmes ne peut pas être prédit par un expert.

6.6 Sécurité du terminal utilisateur

On ne peut pas garantir que l'appareil sur lequel l'utilisateur vote est sécurisé : la connexion n'est pas surveillée, il n'y a pas de virus qui pourrait modifier le vote ou bien envoyer son contenu à un attaquant.

Cependant, on sait bien que ces mêmes utilisateurs utilisent déjà toutes sortes d'applications sensibles (bancaires ...) quotidiennement sur ces mêmes appareils. Mais ce n'est pas une raison pour ne pas le prendre en compte, d'autant que ces applications reçoivent ces mêmes critiques.

6.7 Cible d'attaques

Quelques serveurs qui hébergent un vote important sont une cible bien plus facilement atteignable que des milliers de bureau de vote éparpillés dans le pays. Même dans le cas d'un vote traditionnel à l'université où les assesseurs peuvent réellement voir ce qu'il se passe.

En effet, un petit nombre d'individus avec des moyens peuvent potentiellement fausser significativement un grand scrutin. La contre-mesure du vote traditionnel est, par exemple lors des élections présidentielles, la limite fixée à 1000 votants par bureau de vote. Une fraude mise en

évidence peut invalider ces 1000 votes sans que cela ait des répercussions sur le résultat final.

Une attaque bien plus facile et tout aussi contraignante envers des serveurs est une attaque par déni de service ou DoS (Denial Of Service) qui pourrait rendre inaccessible le site du vote pendant toute la durée du vote.

6.8 Recours

Ces problèmes engendrent un autre problème majeur : la difficulté à apporter des preuves afin de porter une éventuelle fraude ou erreur devant un tribunal. Il n'y a potentiellement pas de trace à mettre en évidence dans le cas d'une erreur informatique et une fraude peut être de taille variable. Le tribunal ne peut alors pas déterminer l'ampleur du problème et décider ou non de la nécessité d'annuler le vote.

C'est un des arguments de Chantal Enguehard, enseignante-chercheuse en informatique à l'Université de Nantes et directrice de recherche à l'Observatoire du vote qui dit : "[des industriels du vote électronique] disent « ça marche bien, la preuve, il n'y a pas contentieux électoraux ». Oui, il n'y a pas de contentieux électoraux parce qu'il est impossible d'apporter quoi que ce soit devant un juge.".[7]

Conclusion

Les systèmes de vote électronique peuvent paraître attrayants aux yeux des organisateurs de scrutins. En effet, ceux-ci sont plus simples à mettre en place que le vote traditionnel qui demande de grands moyens humains et logistiques dès que le nombre de votant augmente. Le vote électronique propose aussi une plus grande flexibilité pour les votants, le vote est ouvert pendant plus longtemps et la contrainte du déplacement n'est plus présente.

Cependant il n'est pas simple de répondre à toutes les attentes que l'on se doit d'avoir pour un des systèmes au centre de la démocratie. Comme nous l'avons vu, en plus d'accentuer certaines problématiques du vote papier, ces solutions en engendrent aussi de nouvelles.

D'un côté, nous avons la solution de Neovote. Ce système étant sous secret défense, ses mécanismes sont complètement cachés au public et ceci pose un très grand problème de confiance qui pourrait engendrer l'illégitimité des résultats. Leur solution est dite homologuée par différents organismes comme le Sénat ou la CNIL mais cela n'a en réalité que peu de valeur puisqu'il ne s'agit pas d'organismes d'homologation. La CNIL déconseillant elle-même l'utilisation du vote électronique par internet pour des votes politiques.

De l'autre côté, nous avons la solution de Belenios. Ce système est complètement ouvert à tous et c'est une première différence de taille avec Neovote. Ceci permet un contrôle du vote de la part de chaque votant et règle une partie des problèmes de confiance. Avec Belenios, on peut nommer plusieurs autorités pour la gestion des serveurs et des différentes étapes critiques du vote.

Il subsiste toutefois les problèmes de compréhension des mécanismes employés. Les notions de cryptographie utilisées ici nécessitent des connaissances en mathématiques et en informatique que tout le monde ne possède pas. Mais il est tout de même possible d'analyser le code utilisé et ainsi de se faire son propre avis quant à la sécurité de leur solution, de plus Belenios s'ouvre ainsi aux examinations des pairs et répond de cette façon au principe de Schneier, un principe important en sécurité informatique.

Malgré tout, des problèmes totalement hors de portée des organisateurs et des prestataires persistent comme les bugs informatiques, les faiblesses dans la sécurité des appareils des utilisateurs et l'augmentation des risques de coercition. A ceci s'ajoute l'incapacité pour une tranche non négligeable de la population d'accéder en autonomie au vote par internet.

À l'opposé, nous avons le vote papier qui possède bien évidemment lui aussi des défauts. Pour preuves les cas avérés de fraudes électorales qui attaquent plusieurs points différents du processus de vote (affaire Tibéri, fraude à la chaussette etc). Ce n'est tout de même pas une raison pour l'abandonner et quelques points d'amélioration sont connus comme ce dont Chantal Enguehard parle sur la publication en ligne des "résultats électoraux détaillés avec le nombre d'émargements, avec le nombre de votes, etc., après les élections"[7]. Ceci permettrait ainsi un contrôle extérieur afin de mieux détecter les erreurs et les tentatives de fraudes.

De plus, les fraudes des votes électroniques sont bien plus compliquées à détecter que celles du vote papier et à celles-ci s'ajoutent les potentiels bugs informatiques, personne ne peut être certain de les empêcher. Ceci freine les possibilités de contentieux électoraux et prive les électeurs et les candidats d'un droit important, celui de pouvoir montrer à la justice qu'une fraude ou une erreur a eu un impact assez grand pour changer le résultat du vote et ainsi le faire annuler.

Le fort abstentionnisme est un sujet très important et qui va le devenir d'autant plus dans cette prochaine période d'élection présidentielle. Nous ne pensons pas que ce problème puisse être résolu en choisissant d'organiser des élections avec un système qui de par sa technicité ou de par la volonté du prestataire se veut opaque et hors de portée de la compréhension des votants.

Cette opacité semble aussi causer des problèmes pour les organisateurs qui se voient faire des choix non conformes sur certains points de sécurité ou d'organisation. C'est ce qui a notamment engendré le problème cité dans ce rapport concernant les votes multiples durant la primaire Populaire en janvier dernier.

Toutes ces problématiques questionnent sérieusement la fiabilité du vote électronique et la conclusion que nous tirons de nos recherches, rejoint celle de la CNIL sur le fait qu'il est très peu conseillé d'organiser un vote électronique pour des élections se voulant sérieuses et voulant respecter ses électeurs et leurs droits en matière d'anonymat et de transparence.

Références

[1] Horn Alexandre. Le vote en ligne de la primaire populaire est-il sécurisé ?, January 2022. https://www.numerama.com/politique/829983-le-vote-en-ligne-de-la-primaire-populaire-est-il-securise.html.

[2] Belenios : Verifiable online voting system. https://www.belenios.org/documentation.html.

[3] Schneier Bruce. "Schneier's Law" - Schneier on Security. https://www.schneier.com/blog/archives/2011/04/schneiers_law.html.

[4] Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239.

[5] Vincent Coquaz. Peut-on vraiment voter plusieurs fois à la «primaire populaire» ? https://www.liberation.fr/checknews/peut-on-voter-plusieurs-fois-a-la-primaire-populaire-20220130_2ZKAHOXEIFBK7G2UKUXSKE746A/.

[6] SSL & Digital Certificates by GlobalSign. https://www.globalsign.com/en.

[7] Étienne Gonnu. 129 - Les enjeux du vote électronique, February 2022. https://www.libreavous.org/129-les-enjeux-du-vote-electronique.

[8] Gilles J. Guglielmi and Olivier Ihl. *Le vote électronique*. LGDJ-Lextenso éditions, Paris, 2015.

[9] Let's Encrypt. https://letsencrypt.org/.

[10] Neovote. https://www.neovote.com/.

[11] Ordinateurs-de-vote.org - Questions fréquentes. https://www.ordinateurs-de-vote.org/-Questions-frequentes-.html.

[12] Thibault Samuel, Delecroix Vincent, and Enguehard Chantal (Université de Nantes). À propos du vote électronique. https://dept-info.labri.fr/~thibault/motion.html.

[13] Legleye Stéphane and Rolland Annaïck. Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base - Insee Première - 1780. https://www.insee.fr/fr/statistiques/4241397.

[14] Vote électronique : préserver la confiance des électeurs. https://www.senat.fr/rap/r13-445/r13-44519.html.

[15] Séléna Laval sur Twitter. https://twitter.com/SelenaCCLaval/status/1465729566614429697.

[16] Critères communs, October 2021. https://fr.wikipedia.org/wiki/Crit%C3%A8res_communs#Niveaux_d%27assurance_EAL.

[17] Fraude électorale, November 2021. https://fr.wikipedia.org/wiki/Fraude_%C3%A9lectorale.

[18] Hardware Security Module, August 2021. https://fr.wikipedia.org/wiki/Hardware_Security_Module.