Intitulé de l'épreuve : Note de synthèse

Nombre de copies :

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

"Sécurisation du vote par correspondance électronique par Internet utilisé pour les français à l'étranger : enjeux et difficultés."

Le vote électronique en France est un sujet débattu depuis la première recommandation en 2003 de la CNIL concernant la dématérialisation des bulletins de vote. Suivra l'article R176-3 du code électoral encadrant le déploiement du vote électronique, en indiquant que si le matériel ou logiciels ne permettent pas de garantir le secret, alors le ministère des Affaires Etrangères peut, après avis de l'ANSSI, annuler le vote.
Se posait déjà la question de sécurisation des outils mis à disposition des citoyens, afin de garantir la séparation de l'identité de l'électeur, et de l'expression de son vote.
Ces exigences et la difficulté pour les mettre en place est toujours - voir encore plus - d'actualité.

1 - Enjeux de la sécurisation du vote électronique

a) Un espoir de relance du processus démocratique

N° A17

[redacted]

Les objatifs sont multiples, ciblant notamment les jeunes électeurs et les français à l'étranger, de recul de l'abstention en permettant de voter depuis chez soi. De coté organisationnel, le fait de moderniser l'organisation des votes apporterait amélioration de la fiabilité des decomptes, mais également une baisse des coûts. Sur ce dernier point on peut noter que la mise en place de la plateforme électronique et son maintien sur quatre années a été à hauteur de 6,78 millions d'euros, avec pour comparaison l'envoi des documents aux français de l'étranger un coût de 3,27 millions d'euros pour les dernières élections législatives.

b) une promesse de campagne.

les nouvelles technologies ont été intégrées dans le programme du président Macron.
Il indiquait récemment qu'il est question de crédibilité et souveraineté nationale face aux problématiques lors de la mise en place du vote électronique en 2017.
D'autres dirigeants politiques, comme monsieur Fillon, s'était déjà engagé par le passé pour un déploiement national du vote électronique jusqu'à là cantonné aux élections professionnels (CE, représentants du personnel) et autres élections d'assemblées générales.
Les détracteurs des nouvelles technologies avancent quand à eux que le vote électronique est plus une stratégie politique et électorale qu'un souhait de mettre à disposition le vote dématérialisé à l'ensemble des

concitoyens du pays.

c) Les français résidants à l'étranger en premières lignes

L'ordonnance 2009-936 permet le vote électronique en suffrage direct pour une élection nationale pour les français établis hors de France. Suivèrent en 2012 les élections législatives et en 2014 les consulaires sur lesquelles donc les français à l'étranger ont pu bénéficier de la mise en place du vote électronique.

d) la sécurisation du vote par correspondance

Les exigences établies par la CNIL sont nombreuses, et balaies un périmetre assez large pour controller au mieux l'ensemble du processus de vote par Internet.

- mesures physiques (contrôle d'accès, liste des personnes habilités) et logiques (pare-feu, contrôle des applications)
- audit du logiciel mis à disposition (contrôle du code source notamment) par un expert indépendant
- reprise des exigences prévues dans le référentiel général de la sécurité (RGS)
- scellement avant le début du scrutin
- confidentialité, chiffrement de bout en bout
- conservation des supports informatiques.

Enfin plus récemment la blockchain est présenté comme une technologie une "arme numérique" permettant de limiter la triche et de fiabiliser l'anonymisation des données.

N° 3.1.7

Malgré le cadre réglementaire et technique déployé en France, de nombreux détracteurs mettent en avant les nombreuses difficultés rencontrées lors des campagnes de test mais également lors de ~~campagne~~ votes réels.

L'exemple le plus récent est l'annulation du vote électronique par le Ministère des Affaires Etrangère lors de l'élection législative de 2017, qui avait fait suite à un avis prononcé en ce sens de la part de l'ANSSI.

Au grand damne de plusieurs personnalités politique, cette décision a été justifiée par plusieurs inégalités au niveau de la sécurité.

II Difficultés de sécurisation du vote électronique

a) un retour arrière général.

Avant de s'attaquer au cas français, notons que de nombreux pays ont soit limité le vote électronique à certaines élections, soit annulé celui ci : la Grande Bretagne, les Etats-Unis, l'Espagne par exemple.

Les difficultés rencontrées sont somme toute similaires

b) un environnement non contrôlé

Partons du principe que le serveur représente dans le processus de vote actuel l'urne classique, et le poste client le bulletin de papier.
Dans ce cadre le canal de transmission échappe à la surveillance des scrutateurs.

Intitulé de l'épreuve : Note de synthèse

Nombre de copies :

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

En découle une problématique de pression éventuelle de l'électeur. D'une manière générale il y a une faible capacité à observer les atteints aux principes d'une élection démocratique.

c) liste des attaques possibles

La liste est longue, et la CNIL indique que celles-ci n'ont pas nécessité d'être complexes pour mettre à mal le vote électronique pour une partie ou l'ensemble des électeurs :

- changement automatique de vote
- annulation des votes
- usurpation d'identité (vol des certificats asymétriques)
- rendre public les votes

Ceci pourrait être possible avec la mise en place d'une trappe (backdoor) dans le code source du logiciel. Un audit est alors nécessaire pour chaque type de machines / logiciels, ce qui représente une grande difficultés comme l'indique Guillaume Poupard, de l'ANSSI.

Des attaquants internes comme externes peuvent plus simplement :

- changement aléatoire des votes (via DDOS)

N° 5.1.7

[redacted]

- intégrer un plug-in dans le navigateur (par une campagne de fishing par exemple) Ceci peut être effectué côté client, mais également côté serveur ce qui serait plus pénalisant encore.

Enfin techniquement, un simple bug n'est pas à exclure.

d) des exemples concrets

Les attaques s'intensifient ces dernières années et comme le souligne l'ANSSI la complexité de celles-ci a fortement augmenté depuis 2012. Des pays plutôt en faveur du vote électronique et de l'e-administration en général (Suisse, Estonie, Lettonie, Corée du Sud) ont connu des piratage de grande ampleur.

En Estonie, une attaque en 2017 imposa au gouvernement de mettre hors réseau une grande partie de son infrastructure pendant 15 jours, en résulte un stockage des données sur différents serveurs et sur différents lieux. Problème en France la CNIL préconise un stockage des données sur le territoire nationale

Enfin l'état intensifie les moyens financiers pour déployer des technologies comme le vote électronique, et s'appuie pour cela sur des prestataires. Cependant la qualité n'est pas toujours au rendez-vous. Malgré un changement (auparavant ATOS puis désormais l'espagnole Scytl) des audits ont démontrés en 2017 que la plate forme mise en place à l'occasion des

N° 6.1.7

élections législatives pouvait être ralentie par une attaque. Les investigations suivantes démontreront qu'une fuite de données a eu lieu sur les serveurs, la suite est désormais connue : l'élection par voix électronique a été annulée.

La sécurisation du vote électronique est plus que jamais primordiale pour garantir des élections démocratiques, et malgré les budgets alloués par le gouvernement des instances comme l'ANSSI, via la voix de son directeur général, sont défavorables en l'état à la mise en place de cette technologie pour les français de l'étranger. De nombreuses corrections doivent être apportées pour redonner confiance aux instances de sécurité du pays, et aux électeurs.

N° 7.1.7.

N°

.../...