COMMUNIQUÉ
Boulogne le 17 mai 2013

LA CNIL REMET EN CAUSE LE VOTE PAR INTERNET

Le 16 mai 2013, la Commission nationale de l'informatique et des libertés (CNIL) publiait une décision du 11 avril dernier de nature à remettre profondément en cause le principe même du vote par internet lors des élections professionnelles.

S'appuyant sur une lecture des dispositions du Code du travail à la lumière de sa recommandation de 2010 à la portée discutable, et dans le cadre d'une position globale qui contrevient clairement aux exigences posées par l'autorité française en charge de la sécurité des données, l'ANSSI[i], la CNIL a donc choisi de prononcer un avertissement à l'encontre d'élections organisées par un client d'Election Europe.

ELECTION EUROPE signale que les orientations ainsi retenues par la CNIL sont, pour certaines, impraticables ou de nature à exposer le vote électronique à plus de risques, et réfute catégoriquement les trois griefs retenus et mettant en cause, premièrement, l'expertise technique indépendante de son logiciel de vote électronique prévue par le Code du travail, deuxièmement, les modalités de transmission des identifiants et mots de passe aux électeurs par courrier, troisièmement et enfin, les modalités de cryptage du bulletin de vote[ii].

Outre que l'essentiel de ces griefs est lié au contexte particulier des élections en cause, ils sont, sur le plan technique, en totale contradiction avec les constats unanimes d'experts agréés par les plus hautes juridictions françaises qui ont eu à connaitre du logiciel d'ELECTION EUROPE. Ils sont aussi contraires aux recommandations catégoriques des Agences gouvernementales de sécurité informatique française ou américaine qui font autorité à l'échelon mondial en matière de sécurité des réseaux.

De plus, nombre de ces griefs impactent l'ensemble des acteurs de la profession, comme par exemple, l'envoi par courrier des codes de vote aux électeurs.

Dans ces circonstances, ELECTION EUROPE entend donc contester la légalité de cette décision et engage un recours en ce sens devant le Conseil d'Etat.

Régis Jamin.
Directeur Election Europe.

Plus d'informations ou nous contacter : www.election-europe.com

[i] En effet, le 19 avril 2013, l'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information Française, reprenait dans une note technique(*), la mise en garde du US-CERT, Agence de Sécurité Informatique des Etats-Unis du 10 janvier 2013 qui recommandait de désinstaller Java de tous les postes Internet suite aux millions de piratages constatés de part le monde. Le Conseil Constitutionnel reconnaissait par ailleurs dans sa décision du 15 février 2013 que des bulletins électroniques piratés avaient été émis lors des législatives de juin 2012 avec une solution de vote internet utilisant Java sur les postes des votants.
(*) http://www.ssi.gouv.fr/IMG/pdf/NP_Securiser_JRE_NoteTech.pdf
L'ANSSI conclut dans sa dernière recommandation : « *Lorsque cela s'avère réalisable simplement, remplacer les applications légères Java par des applications alternatives. Ne plus nécessiter les modules complémentaires Java dans les navigateurs Web des postes utilisateurs permet de réduire notablement leur surface d'attaque.*
Attention toutefois à ne pas remplacer un environnement d'exécution Java au profit d'une autre technologie nécessitant des modules complémentaires apportant potentiellement d'autres vulnérabilités. »

[ii] La CNIL recommande que le chiffrement du bulletin soit géré uniquement sur le poste du votant donc par téléchargement d'un logiciel de type applet Java ou Javascript et que le bulletin chiffré sur le poste du votant soit transmis en l'état sur le serveur de vote.
La solution Election-Europe est effectivement différente car elle utilise un triple mécanisme de chiffrement et de signature électronique du bulletin sans recours au téléchargement sur le poste du votant.
Election-Europe avait estimé il y a plus de dix ans que faire reposer toute la sécurité du vote sur un logiciel téléchargé sur le poste du votant pouvait être dangereux car c'est le seul maillon de la chaîne de traitement du vote que l'on ne peut contrôler.
La réalité des cyber-attaques massives via applets « java » constatées en ce début d'année 2013 ont donc donné raison à Election-Europe.
La recommandation CNIL d'utiliser un logiciel téléchargé qu'il soit une applet java ou un code javascript pour assurer des fonctions de sécurité dans une application web est donc aujourd'hui clairement en contradiction avec les demandes expresses des diverses Agences de Sécurité Informatiques Gouvernementales.