Le vote est-il un service dématérialisable ?

Hervé Suaudeau

▶ **To cite this version:**

Hervé Suaudeau. Le vote est-il un service dématérialisable ?. Journées RESeaux (JRES) de l'enseignement et de la recherche 2017, Nov 2017, Nantes, France. hal-02071766

HAL Id: hal-02071766
https://hal.science/hal-02071766

Submitted on 18 Mar 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Le vote est-il un service dématérialisable ?

Hervé Suaudeau
CNRS UMR 8119
45, rue des Saint-Pères
75 270 Paris cedex 06

Résumé

Le vote dématérialisé possède des avantages apparents séduisants et provoque un engouement des nouveaux responsables politiques nationaux. Pourtant certains responsables informatiques de poids comme le directeur de l'ANSSI, ou des scientifiques ont pris nettement leurs distances. Face aux cyber-menaces, le vote par internet des Français de l'Étranger a même été supprimé le 6 mars 2017.

Pour tenter de démêler ces contradictions, nous essaierons de répondre aux questions suivantes :

- *Face à des technologies forcément imparfaites mais apportant de nouveaux services, quel est le rapport bénéfice / risque ?*
- *Pourquoi les améliorations techniques buttent-elles contre le problème intrinsèque à la dématérialisation de systèmes anonymes ?*
- *Pourquoi le logiciel libre, la vérification formelle ou la technologie blockchain ne peuvent probablement pas nous sortir de cette situation ?*
- *Sachant cela, quelles précautions ou attitudes peuvent avoir les ASR et développeurs chargés dès aujourd'hui de mettre en place des services de vote informatisés ?*

Mots clefs

Sécurité informatique, vote électronique, vote par Internet, vérifiabilité, anonymat, dématérialisation

1 Introduction

En 2017, la France sort d'une séquence de vote politique importante pendant laquelle plus d'un million d'électeurs ont eu la possibilité de voter électroniquement pour les élections présidentielles et législatives [1]. Pourtant, il pèse toujours des soupçons sur les systèmes dématérialisés impliqués dans les opérations électorales. Ainsi, certains responsables informatiques comme le directeur de l'ANSSI [2] ont pris leurs distances avec le vote électronique. Le vote par internet des Français de l'Étranger, initialement autorisé pour les élections législatives de mai et juin 2017, a même été supprimé le 6 mars 2017 pour éviter d'offrir à des services étrangers une capacité supplémentaire d'ingérence.

Cette situation peut amener les ASR et développeurs chargés parfois de mettre en place des services de vote informatisés de moindre importance à s'interroger. Chacun à son niveau peut ainsi apporter une réflexion, bien sûr technique, mais aussi éthique et démocratique à cette question.

1. Environ 1,3 millions d'électeurs sont inscrits dans des communes où des machines à voter sont utilisées (présidentielles et législatives) et 1,07 millions de Français de l'Étranger auraient eu la possibilité d'élire par internet les 11 députés qui les représentent en 2012 si cette modalité de vote avait été maintenue.
2. https://www.nextinpact.com/news/102944-le-numero-l-anssi-defavorable-au-vote-electronique.htm

2 Qu'est-ce qu'un vote dématérialisé ?

Même si notre communauté n'est généralement confrontée qu'à la question du vote par internet, il est utile de connaître les autres systèmes de vote entièrement ou partiellement dématérialisés utilisés en France car ces techniques sont très différentes :

— Les **machines à voter** sont des ordinateurs placés dans les bureaux de vote afin d'enregistrer les suffrages. En 2017, environ 1,3 millions d'électeurs devaient utiliser ces dispositifs lors des élections politiques dans une soixantaine de communes en France. En 2007, la liste des communes autorisées à utiliser ces ordinateurs de vote a été gelée.

— Les **boîtiers sans fil des assemblées générales ou des conseils d'administration** sont des outils de vote dématérialisé (supposé anonyme) souvent oubliés de ceux qui dénoncent les abus de la dématérialisation des scrutins. Pourtant nombre de décisions importantes de notre pays sont prises à travers l'utilisation de ces systèmes dans les instances de décision de syndicats, d'actionnaires, d'assemblées économiques ou d'organisations de poids.

— Les **pupitres électroniques des députés et sénateurs** sont les systèmes de vote électronique qui sont paradoxalement le moins sujet de controverse. En effet, bien que les décisions les plus importantes de notre pays puissent être potentiellement recueillies par ce système dématérialisé, celui-ci reste parfaitement vérifiable car le vote n'est pas secret. Il n'est pas rare d'ailleurs que certains parlementaires, consultant la liste des suffrages de chaque votant, souhaitent *a posteriori* modifier l'enregistrement de leur vote.

— Le **vote par correspondance dépouillé par scanner** (appelé aussi vote par correspondance hybride) est aujourd'hui vécu comme l'équivalent du vote par correspondance avec double enveloppe (voir exemple sur figure 1). Pourtant, ce sont bien des machines qui lisent les codes barres identifiant l'électeur, lisent la nature du vote dans une case à cocher ou sur une étiquette et effectuent le comptage total. Bien que matérialisé sur papier, ce vote est bien à traitement informatique et incorpore donc (au moins pour une bonne part) les problématiques inhérentes à la dématérialisation des scrutins [3].

3 L'évaluation des bénéfices / risques

Comme pour tout projet de dématérialisation, les responsables informatiques doivent évaluer la pertinence de la mise en place d'une solution électronique par rapport à un procédé traditionnel. Ils doivent donc faire le tri entre les qualités réelles et prétendues couramment répétées à propos des systèmes de vote dématérialisés :

— Le vote par internet augmenterait la **participation** : aucune étude ne vient corroborer cette affirmation souvent répétée mais les contre-exemples ne manquent pas [4]. En réalité, le vote sur ordinateur, plutôt que de faciliter les possibilités de s'exprimer, peut rendre l'élection moins palpable, impossible à être démontrée fiable à l'électeur, et finir par instaurer une certaine méfiance pouvant entraîner un recul important de la participation.

3. On peut remarquer qu'il serait aisé de vérifier manuellement les résultats électoraux énoncés à l'issue d'un tel vote mais que cette possibilité n'a, à notre connaissance, jamais été mise en place et qu'elle n'est présente dans aucun texte juridique.

4. Deux exemples dans la communauté éducation/recherche de la chute de la participation suite à l'installation du vote par internet :

— Baisse de 26 % aux élections du CA du CNRS en 2009 (27 342 inscrits).

— Baisse de 36 % pour les élections professionnelles dans l'éducation nationale en 2011 (1 038 294 inscrits) (baisse de 32 % en 2014 par rapport à au précédent vote papier).

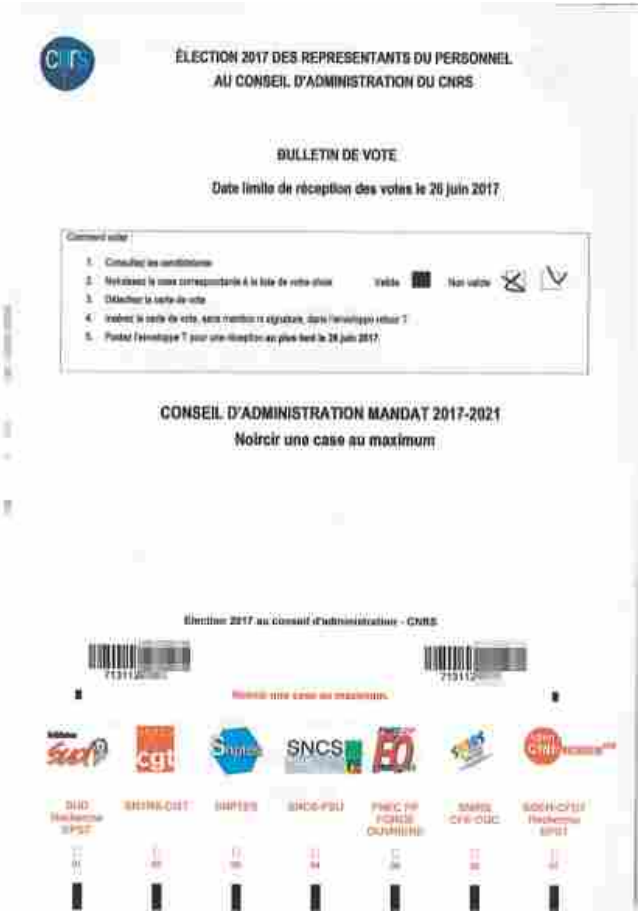

Figure 1 - Exemple de bulletin de vote par correspondance dépouillé par scanner

— Le vote par internet ferait baisser les **coûts** : là encore, aucune étude ne permet de corroborer cette affirmation et les exemples que nous pouvons tirer des expériences dans la communauté éducative nous inciteraient à penser le contraire [5].

— Le vote par internet aurait un meilleur **bilan écologique** : cet argument encore utilisé par les vendeurs de systèmes de vote est aujourd'hui en perte de vitesse, car nous savons désormais que l'impact environnemental des opérations dématérialisées peut parfois être très élevé et qu'il faut aussi lui rajouter le cycle de vie des matériels nécessaires (construction, utilisation de matériaux épuisable, recyclage…). Cet argument peut aussi paraître dérisoire face à la quantité de papier que nous utilisons encore pour des motifs plus futiles que les décisions démocratiques [6].

— Le vote par internet serait **moderne** : cet argument est le premier évoqué par les personnels politiques [1]. Il fait partie des sophismes de l'appel à la modernité. Ils ne peuvent être pris en compte dans un débat rationnel.

— Le vote par internet **facilite l'accès aux élections** pour les petits candidats : c'est un argument réel qu'on entend peu souvent bien qu'il entraîne un progrès démocratique.

— Le vote par internet serait **facile à mettre en œuvre** : en fait il existe une complexité à la fois juridique

5. À l'installation du vote par internet au CNRS le coût est passé de 40K€ (élection CA 2005) à 140K€ (élections CA 2009). Ce coût de plus de 15€ par vote a poussé à l'abandon de cette solution par le CNRS en 2012 (source rapport « Bilan vote électronique par internet » – 25 juin 2012 – Réunion DRH OS CNRS), mais aussi suite à 2 ans de recours électoral.

6. Chaque foyer reçoit 30 kg de papier de publicité non adressée par an (source ADEME 2015)

et technique.

— Le vote par internet serait **facile à utiliser** : il n'existe pas de tests d'utilisabilité.

— Le vote par internet **facilite les comptages complexes** : c'est un argument réel mais il ne faut pas oublier qu'un comptage relativement complexe est aussi possible manuellement s'il est bien organisé, d'autant plus qu'il permet éventuellement d'éviter des élections à plusieurs tours.

— Le vote par internet **limiterait la fraude** : il est ici raisonnable de penser le contraire si l'on considère les acteurs qui ont intérêt à cette fraude. En effet, ce ne sont pas tant les électeurs qui sont motivés à frauder mais surtout les candidats, les mafias, les groupes terroristes, les États et leurs services spéciaux. La dématérialisation offre à ces entités motivées pour investir des sommes importantes [7], une surface d'attaque bien plus forte car centralisée et par des vecteurs facilement disponibles et souvent indétectables. L'arrêt du vote par internet des Français de l'Étranger en 2017, ou le retour du comptage entièrement manuel des scrutins aux Pays Bas depuis mars 2017, sont des exemples concrets de la prise en charge de ces menaces. Par ailleurs, il existe plusieurs exemples de votes par internet dont la faiblesse a été démontrée à l'issue de tests de hacking [3] ou alors qu'ils étaient en usage [4].

— Le vote par internet peut augmenter les **risques juridiques** : un vote électronique, du fait de son impossibilité à être démontré fiable à l'électeur, peut susciter des volontés de multiplier les recours. Il est donc important de bien circonscrire ce type de risque. L'e-vote est un traitement de données à caractère personnel des votants, qu'il convient de protéger d'autant plus qu'il s'agit de données sensibles. La responsabilité de l'organisateur du vote est ici pleinement engagée notamment devant la CNIL, en cas de non-respect des obligations liées à la loi Informatique et Libertés même en présence d'un sous-traitant [8]. Par ailleurs, si le scrutin se déroule dans le cadre d'une élection professionnelle, d'autres contraintes supplémentaires se rajoutent, telle une expertise préalable indépendante, limitée au serveur et destinée à vérifier que les exigences légales sont bien remplies par le dispositif technique.

Les ASR doivent aussi prendre en compte les inconvénients métiers auquel tout informaticien pense naturellement (attaques, vulnérabilités, bugs…) mais ceux-ci ne doivent pas occulter l'argument éthique central : **le vote électronique entraîne la fin de la transparence directe du fait de l'impossibilité pour l'électeur, mais aussi pour quiconque, de pouvoir contrôler directement la sincérité de ce type de scrutin.**

Cet argument démocratique, qui conditionne la confiance des électeurs, et donc la légitimité des élus, est hélas souvent oublié lors de l'évaluation des bénéfices/risques bien qu'il soit à lui seul suffisamment prépondérant pour envisager d'écarter le vote électronique sans avoir besoin de considérations techniques [9].

4 Les problèmes de fond liés à la dématérialisation

Le vote électronique porte en lui plusieurs problématiques fondamentales dues à la dématérialisation partielle ou totale. Ces problématiques sont parfois complexes à appréhender mais leurs conséquences sont souvent rédhibitoires quant à l'usage du vote dématérialisé anonyme. Nous aborderons trois de ces notions.

7. Ruud Verbij a décrit une méthode de fraude [2] qu'il évalue à 40 000$ par siège obtenu au parlement estonien ou l'élection se fait par internet.

8. Ex : En 2013 l'entreprise Total a été épinglé par la CNIL pour défauts de sécurité dans un vote électronique alors qu'elle utilisait pourtant une solution standard du marché.

9. Il ne faut pas négliger non plus que des électeurs peuvent hésiter à exercer pleinement leur liberté de vote car ils utilisent un dispositif qui collecte à la fois leur intention de vote et leur identité. Dans cette situation, certains électeurs qui doutent du respect du secret du vote vont émettre un choix plus consensuel que celui qu'ils auraient exprimé s'ils avaient voté en toute liberté.

4.1 Incompatibilité entre la vérifiabilité des votes dématérialisés et l'anonymat

4.1.1 Le théorème

Cette problématique est celle qui a la conséquence la plus importante, et est probablement la plus complexe à comprendre dans le détail. Les travaux de Chevalier-Mames et al. [5] ont en effet abouti à démontrer pourquoi il y a incompatibilité formelle entre la vérifiabilité des votes dématérialisés et l'anonymat, l'anonymat étant la rupture de tout lien entre un vote et l'électeur qui en a fait le choix. Bien que la démonstration de leur théorème soit difficile d'accès pour un non spécialiste, la conclusion de l'article scientifique est sans appel (traduction personnelle) [10] :

> « En conclusion, nous avons montré que les systèmes de vote ayant les caractéristiques habituelles ne peuvent pas vérifier les notions de sécurité fortes toutes en même temps : nous ne pouvons pas parvenir simultanément à la vérifiabilité universelle [11] du décompte des voix et à la confidentialité inconditionnelle des votes ou à la 'receipt-freeness' » *(l'absence de preuve de son vote protège l'électeur contre la coercition)*.

4.1.2 Les contestations du théorème

On comprendra, vus les enjeux industriels, que les résultats de Chevallier-Mames et al. puissent être discutés.

Certaines critiques [6] réduisent les exigences démocratiques nécessaires en dessous de celles d'un vote papier afin d'y parvenir. Des protocoles [7][8][9] indiquent atteindre simultanément la vérification universelle et l'anonymat, mais nécessitent des conditions préalables inacceptables au point de vue démocratique (mise en place de tiers de confiance) ou irréalistes dans l'état actuel des connaissances (canaux parfaitement anonymes).

Certaines méta-analyses [10] affirment que la vérifiabilité et l'anonymat sont possibles avec des protocoles déjà décrits. Outre que ces travaux souffrent des biais déjà signalés, ils partent de conditions peu réalistes comme l'*a priori* de fiabilité totale du poste client (exempt de bug ou de malware qui pourraient espionner et/ou altérer les votes sans avoir besoin d'interférer avec les protocoles). De plus ils ne résolvent pas la problématique fondamentale de parvenir à convaincre l'électeur de la fiabilité du scrutin, contrairement à un vote à continuité matérielle. Cette absence de vérification tangible pour l'électeur a pourtant des conséquences importantes que nous verrons en partie 4.2.

4.1.3 Conclusion

Les travaux de recherche doivent être poursuivis mais les conclusions du théorème de Chevallier-Mames et al. perdurent dans les conditions actuellement imaginables de mise en place du vote électronique.

Nous pouvons en conclure qu'en l'état actuel des connaissances un système de vote (acceptable et réalisable) ne peut pas être dématérialisé et se prévaloir d'être à la fois anonyme et vérifiable (voir figure 2).

4.2 La « brisure de légitimité » entraînée par la dématérialisation

Ce concept est plus simple à appréhender. Je l'ai introduit lors de mon audition en 2007 auprès du groupe de travail « machines à voter » du Ministère de l'Intérieur, afin de faire comprendre, aux fonctionnaires

10. « As a conclusion, we have shown that voting systems with usual features cannot simultaneously achieve strong security notions : we cannot achieve simultaneously universal verifiability of the tally and unconditional privacy of the votes or receipt-freeness. »

11. La vérification universelle est une notion de sécurité qui vise à empêcher les autorités électorales malhonnêtes de tricher pendant le calcul du décompte.

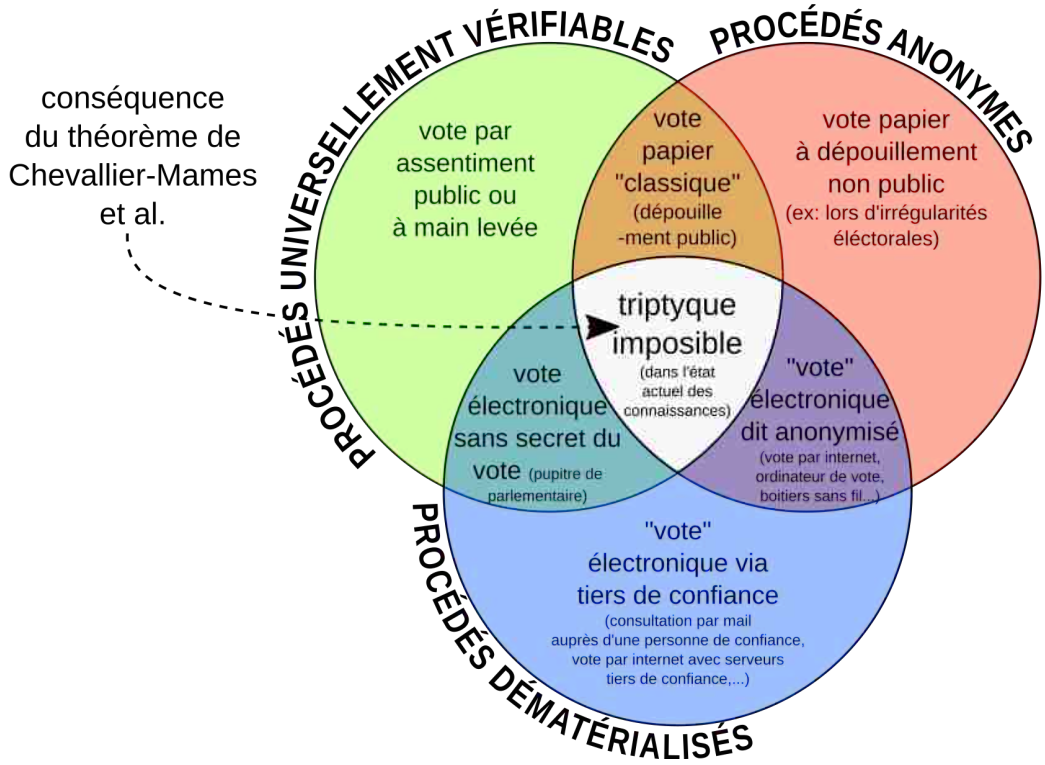

Figure 2 - Classement de différents systèmes de vote en fonction de leurs propriétés et conséquence du théorème de Chevallier-Mames et al.

qui doivent exercer l'autorité de l'État, que la dématérialisation des votes est susceptible d'amoindrir la légitimité des élus.

En effet, un processus électoral démocratique doit, par construction, susciter la confiance. Sans celle-ci, le vote ne peut pas jouer son rôle social d'acceptation de la décision majoritaire. Les personnes soutenant un candidat perdant doivent être convaincues que le résultat est sincère pour accepter leur défaite et considérer le gagnant comme légitime. De cette conviction dépend directement la légitimité de l'élu.

Cette conviction peut être fondée lorsque le vote est opéré avec des urnes transparentes et un dépouillement public. Les électeurs motivés ou les assesseurs ont ainsi la possibilité de vérifier la continuité physique du scrutin durant toute la journée (en veillant à ce que le contenu de l'urne ne soit pas modifié illicitement) puis assister au dépouillement et être ainsi convaincu que le vote s'est bien déroulé sans avoir à reposer leur vérification sur la confiance d'un tiers.

Contrairement à un vote observable avec continuité matérielle, la médiation introduite par la dématérialisation rend impossible une démonstration tangible pour l'électeur de la fiabilité du processus. L'e-votant n'a plus de preuve palpable que le scrutin s'est convenablement déroulé et, faute de conviction, est obligé de croire ce bon déroulement de l'élection bien qu'aucune preuve ne puisse lui en être apportée. En effet nul ne peut assurer un contrôle du bon déroulement d'une élection électronique (les expertises se déploient en dehors des périodes de vote, et ne peuvent donc porter sur des élections réelles). L'électeur se voit ainsi retirer le droit de contrôle de l'élection constituant un recul démocratique fondamental. Ce recul provoquera des doutes quant à la justesse des résultats électoraux et donc des doutes quant à la légitimité des élus.

La légitimité de ceux qui doivent représenter les électeurs est ainsi brisée par cette dématérialisation (voir figure 3). Cette brisure de légitimité entraîne mécaniquement une crise d'autorité, à laquelle un fonctionnaire du ministère de l'intérieur qui doit exercer cette autorité est immédiatement sensible.

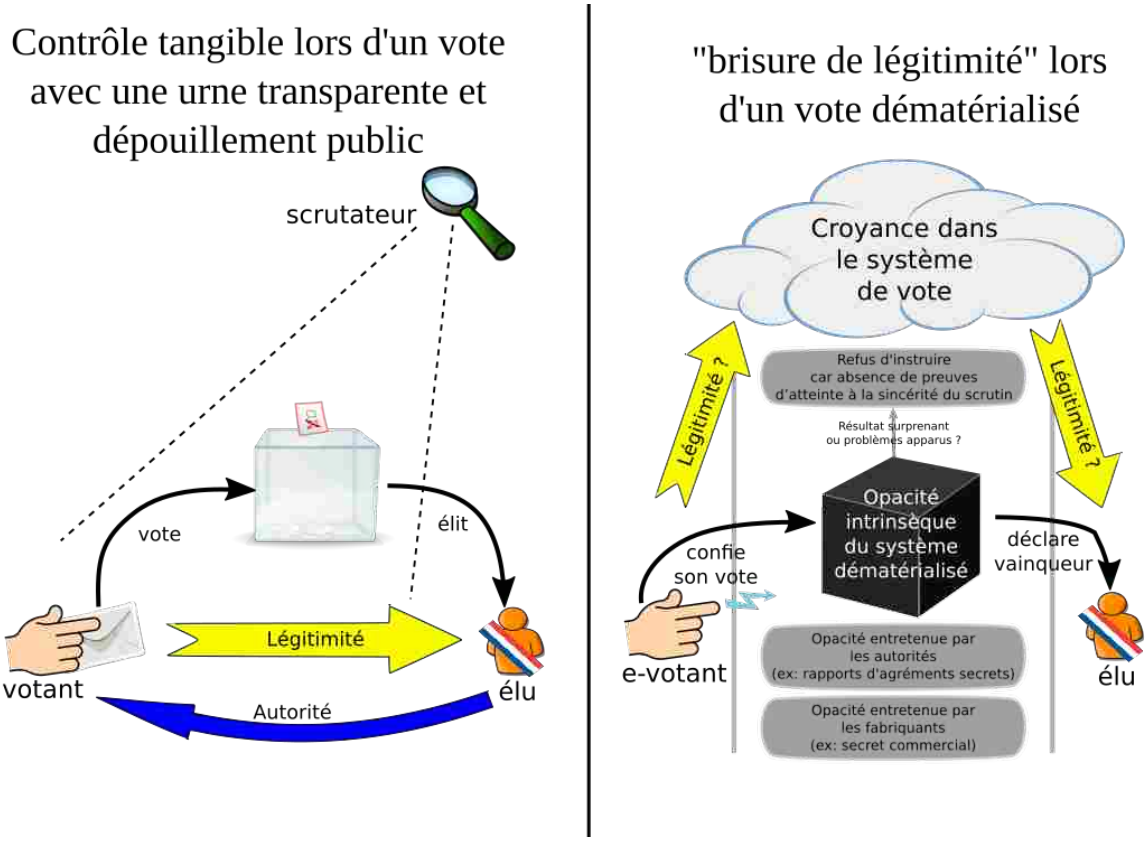

Figure 3 - La légitimité est assurée en vote papier par un contrôle tangible du vote. Avec le vote dématérialisé, l'absence de contrôle direct du vote brise cette légitimité.

5 Biais de confusion des propriétés entre objets réels et avatars

Enfin pour pouvoir appréhender plus complètement la situation, il faudra comprendre ce qu'on pourrait appeler « le biais de confusion des propriétés entre objets réels et avatars » qui est souvent rencontré notamment chez nombre de décideurs (législateurs, magistrats, directeurs d'établissement, etc.) et à l'origine de fausses croyances au sujet du vote électronique. Ce biais revient à prêter les mêmes propriétés aux objets matériels qu'à leur représentation informatique (voir figure 4). Vérifier que « l'urne est vide », n'est ainsi pas la même chose que de regarder une représentation sur écran d'un compteur (compteur fourni de plus par un programme dont on n'a pas l'assurance de la conformité ni de l'absence de bugs ou de failles). Cette confusion est parfois entretenue jusque dans la réglementation [12] ou dans la mise en place de procédures de contrôle de scrutins (voir figure 5).

Confondre la représentation informatique d'un processus et son processus initial reviendrait à croire que l'on pourrait se brûler avec l'image d'un feu sur un écran. Or chacun sait que lorsque l'image du feu est numérisée, sa représentation sur écran perd sa capacité à chauffer. Il en est de même pour le processus électoral qui, une fois dématérialisé, change de nature : il est erroné de lui attribuer automatiquement les mêmes propriétés que les objets matérialisés sauf à tomber dans cette confusion.

12. Ex : les membres du bureau de vote doivent constater en début de scrutin « l'absence de bulletins de vote dans la machine » ; selon l'arrêté du 17 novembre 2003 portant approbation du règlement technique fixant les conditions d'agrément des machines à voter.

Figure 4 - « La trahison des images » de Réné Magritte. Ceci n'est effectivement pas une pipe mais une représentation de cet objet et elle n'a pas les mêmes propriétés que l'objet matériel (ex : impossible de griller quelques brins avec ce tableau. En revanche, on peut le rouler et le dérouler alors qu'il n'est pas possible de rouler une véritable pipe sans la casser).

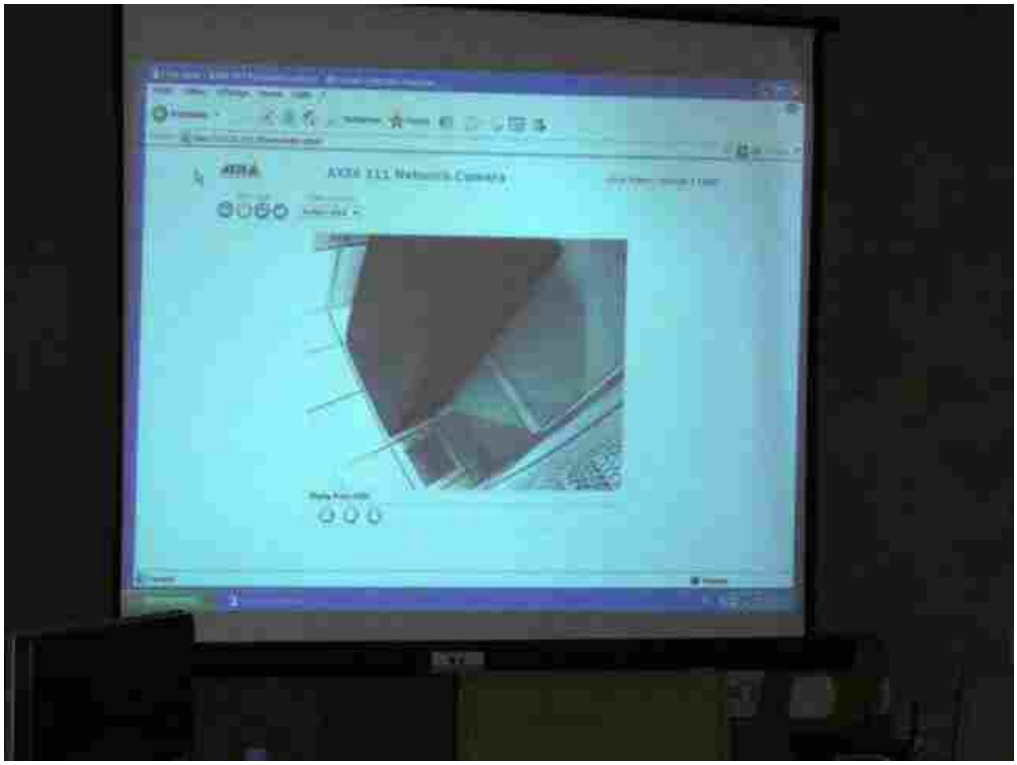

Figure 5 - Exemple de cette confusion de propriété entre urne physique et « urne électronique » : lors du vote par Internet de l'Assemblée des Français à l'Étranger en 2006, les organisateurs n'ont permis aux scrutateurs que de pouvoir regarder le serveur central en guise de toute surveillance du scrutin (comme si cette surveillance était analogue à celle d'une urne transparente dans un bureau de vote). Pire, cette surveillance n'était même pas directe mais était opérée au travers de la diffusion d'images d'une caméra placée dans la salle des serveurs inaccessible aux membres du bureau de vote (photo prise par un assesseur).

6 Des technologies peuvent-elles sauver l'e-vote ?

Voici quelques technologies parfois présentées comme pouvant rendre le vote électronique aussi sûr et démocratique que le vote papier :

- Le **logiciel libre**, comme le confirme Richard Stallman [13], n'est pas une solution suffisante notamment parce qu'un dispositif de vote électronique n'apporte pas la garantie que ses sources de bout en bout soient bien vierges de toute modification par rapport au code de référence.
- Les **preuves formelles de code** ont les mêmes inconvénients (outre qu'elles sont généralement limitées à des programmes assez courts). L'électeur présent devant un système de vote n'a ainsi aucune garantie que le code testé formellement est bien celui présent dans le dispositif.
- Le **chiffrement homomorphe, la cryptographie par canal quantique, les mix-net** et tout procédé permettant de sécuriser une partie du traitement ne règlent pas les problèmes de fonds évoqués plus haut, mais surtout ne protègent pas les parties les plus fragiles de la chaîne de traitement (comme le poste client en vote par internet qui peut être attaqué par des chevaux de Troie de type man-in-the-browser tel Zeus qui peuvent même modifier l'interface utilisateur à la volée).
- La technologie de **blockchain**, malgré les ouvrages qui y voient l'avenir du vote par internet [11], comporte les mêmes problématiques car elle ne peut opérer que d'une partie de la chaîne de traitement. Elle n'a pas non plus de moyen de convaincre un électeur de la sincérité des opérations. En outre elle porte intrinsèquement le danger majeur de révélation du contenu intégral des votes le jour où l'un des protocoles de chiffrement est cassé, car elle est conçue pour rester publique à long terme.

Pour conclure, il est souvent reconnu qu'aucune technique d'anonymisation n'est théoriquement infaillible [14] et les fonctionnalités des protocoles des votes électroniques actuellement proposés ont des limitations importantes au regard de la variété des vulnérabilités de sécurité. Notamment, le risque de ré-identification est à prendre en compte en matière électorale. Il peut avoir des conséquences graves y compris longtemps après un scrutin si par exemple la nature des votes de chacun était révélée suite à l'exploitation d'une faille, nouvellement découverte, qui concernerait un ancien enregistrement, obtenu de manière légale ou pas.

7 Conclusion : quelles solutions de dématérialisation ?

À l'image de ceux qui pensent résoudre la crise climatique par la géo-ingénierie, nous pouvons tomber dans certains biais techno-optimistes et penser résoudre la crise démocratique, à laquelle nos sociétés sont actuellement confrontées, par la dématérialisation du vote. Il peut être spontané de penser pouvoir améliorer les choses par la mise en place de nouvelles et intéressantes fonctionnalités facilitées par l'automatisation des process (multiplication des scrutins, utilisation de méthodes de comptage plus justes, « démocratie liquide »…). Hélas la réponse à cette crise démocratique ne peut pas être – dans l'état actuel de nos connaissances – cette fuite en avant. Au contraire le remède aggraverait la maladie, car la dématérialisation peut empirer la défiance de l'électeur, en rendant opaque ce qui doit être transparent.

Les votes papiers, bien qu'étant loin d'être parfaits, apportent une solution forcément plus simple, « low-tech » et juridiquement plus sûre au problème complexe de la consultation démocratique. On portera à ce propos une attention à certaines études de Chantal Enguehard qui comparent les défauts et qualités du vote par internet et du vote par correspondance [12][13].

La responsabilité de chacun est ici de ne pas banaliser ce concept impossible – dans l'état actuel de nos connaissances – de vote dématérialisé, y compris pour des élections à « faible enjeux », car la généralisation de ces nouveaux usages « par le bas » auront potentiellement des conséquences politiques ou sociales

13. Richard Stalmann : « I think that computerized voting is dangerous, and that the danger cannot be prevented by using only free software ».

14. Ex : rapport d'information du Sénat sur l'open data et la protection de la vie privée qui approuve les propos de Claude Kirchner, chercheur INRIA. http://www.senat.fr/rap/r13-469/r13-4697.html

importantes. *A minima*, il faut refuser l'usage du mot *vote* pour tous ces systèmes qui proposent des fonctionnalités, que l'on peut reconnaître innovantes, mais étrangères aux concepts démocratiques auxquels le mot *vote* se rattache. Notre communauté, comprenant les enjeux de la dématérialisation, peut faire ici de la pédagogie auprès de nos décideurs et autorités pour leur expliquer que tout n'est pas dématérialisable et rappeler que l'écran n'est qu'une représentation de la réalité et non la réalité elle-même. Des institutions, telle l'université de Nantes (voir annexe p.10), sont capables de prendre conscience de cela.

En résumé, telle l'image de la flamme sur l'écran qui perd la propriété de pouvoir nous brûler, le process de vote une fois dématérialisé perd ses propriétés démocratiques. À l'heure actuelle, en matière de vote anonyme, la meilleure dématérialisation est donc celle qui n'existe pas.

Annexe : motion de l'université de Nantes

Voté par le comité technique de l'Université à l'unanimité le 25 novembre 2014 :

> « Depuis plusieurs années, l'usage du vote électronique se développe en France dans le cadre d'élections pour lesquelles le secret du vote est requis. Il s'agit de machines à voter pour des élections ou référenda politiques, ou encore du vote par voie électronique (vote par internet) pour des élections politiques ou professionnelles. L'Université de Nantes, contribuant à la politique nationale de la recherche et du développement technologique, a pour mission d'apporter son expertise aux politiques publiques. Dans cet esprit, le Comité Technique de l'Université de Nantes rappelle que
>
> — le vote électronique reste un champ de recherche actif, en particulier en ce qui concerne le respect simultané du secret du vote et de la sincérité du vote
>
> — il n'existe actuellement aucun outil scientifique qui permette de vérifier, pendant son fonctionnement, qu'un système de vote électronique respecte à la fois le secret du vote et la sincérité des élections.
>
> Aussi, le Comité Technique de l'Université de Nantes déconseille l'usage de systèmes de vote électronique pour les élections et référenda nécessitant un scrutin secret et anonyme. »

Bibliographie

[1] Chantal Enguehard. La controverse des machines à voter en france. *Ecole des Hautes Études en Sciences Sociales*, Mémoire de master 2, 2011.

[2] Ruud Paul Verbij. Dutch e-voting opportunities. risk assessment framework based on attacker resources. *University of Twente*, Master thesis, 2014.

[3] Alex Halderman. Hacking the dc internet voting pilot. *Freedom to Tinker (blog) Oct*, 5 :2010, 2010.

[4] J Alex Halderman et Vanessa Teague. The new south wales ivote system : Security failures and verification flaws in a live online election. Dans *International Conference on E-Voting and Identity*, pages 35–53. Springer, 2015.

[5] Benoît Chevallier-Mames, Pierre-Alain Fouque, David Pointcheval, Julien Stern et Jacques Traoré. On some incompatible properties of voting schemes. *Towards Trustworthy Elections*, 6000 :191–199, 2010.

[6] Alireza Toroghi Haghighat, Mohammad Ali Kargar, Mohammad Sadeq Dousti et Rasool Jalili. Minimal assumptions to achieve privacy in e-voting protocols. Dans *Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on*, pages 1–5. IEEE, 2013.

[7] Ari Juels, Dario Catalano et Markus Jakobsson. Coercion-resistant electronic elections. Dans *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 61–70. ACM, 2005.

[8] Tal Moran et Moni Naor. Receipt-free universally-verifiable voting with everlasting privacy. Dans *Crypto*, volume 4117, pages 373–392. Springer, 2006.

[9] Tal Moran et Moni Naor. Split-ballot voting : everlasting privacy with distributed trust. *ACM Transactions on Information and System Security (TISSEC)*, 13(2) :16, 2010.

[10] Koh Eng Meng et Wang Guan Yu. A survey on electronic voting. *CS2107-Semester IV, 2012-2013*, page 69.

[11] S. Loignon. *Big Bang Blockchain : La seconde révolution d'internet*. Tallandier, 2017.

[12] Chantal Enguehard. Analyse des vulnérabilités de trois modes de vote à distance. *Legalis. net*, 3 :13–31, 2008.

[13] Chantal Enguehard et Rémi Lehn. Vulnerability analysis of three remote voting methods. *arXiv preprint arXiv :0908.1059*, 2009.

Éléments de contribution de Hervé Suaudeau

— Chargé de mission de mise en place d'un vote électronique des représentants de l'Institut de Neuroscience et Cognition (2009).

— Membre de la direction nationale de Ordinateurs-de-Vote.org « Citoyens et informaticiens pour un vote vérifié par l'électeur ».

— Mandataire d'un candidat à une primaire par vote électronique pour la présidentielle de 2012.

— Expérience de terrain quant au contentieux électoral pour des élections dématérialisées depuis 2008.

— Vulgarisation sur le sujet du vote électronique (conférences Pas Sage En Seine-HSF 2016, Ligtning talk JRES 2015, BoF JRES 2011, AIDCM 2011).