ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête concernant l'organisation des élections en France

Jeudi
6 février 2025
Séance de 9 heures 45

Compte rendu n° 10

SESSION ORDINAIRE DE 2024-2025

Présidence de
M. Thomas Cazenave,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures quarante-cinq.

M. le président Thomas Cazenave. Madame Véronique Cortier, monsieur Pierrick Gaudry, vous êtes directeurs de recherche au Centre national de la recherche scientifique (CNRS), au sein du laboratoire lorrain de recherche en informatique et ses applications (Loria). Vous avez publié en 2022, aux éditions Odile Jacob, un ouvrage intitulé *Le Vote électronique. Les défis du secret et de la transparence* ; vous avez également contribué à créer le logiciel de vote électronique Belenios. Vous portez à ce titre un regard à la fois théorique et pratique sur ces questions qui sont au cœur de nos travaux.

L'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter serment de dire la vérité, toute la vérité, rien que la vérité.

(Mme Véronique Cortier et M. Pierrick Gaudry prêtent successivement serment.)

Mme Véronique Cortier, directrice de recherche au CNRS. Mes recherches portent principalement sur les questions de sécurité informatique. Je m'intéresse aux protocoles de sécurisation sur internet, notamment aux protocoles de vote électronique. J'essaie de développer des outils d'analyse des systèmes de vote – déjà déployés ou en cours de déploiement, en Suisse ou en France par exemple, mais aussi des systèmes plus théoriques, étudiés dans un cadre académique. Vous l'avez rappelé, nous proposons la plateforme en ligne Belenios, utilisée chaque année pour quelques milliers d'élections. Nous collaborons régulièrement avec des entreprises, aussi bien en France qu'à l'étranger. Nous discutons avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) ; nous avons été tiers de confiance pour les élections législatives de 2022, afin d'essayer d'apporter plus de vérifiabilité et de transparence.

M. Pierrick Gaudry, directeur de recherche au CNRS. Mes recherches initiales portaient plutôt sur la cryptographie et la théorie des nombres. Je travaille sur le vote électronique en collaboration avec Mme Cortier depuis une douzaine d'années, de façon théorique mais aussi avec une volonté de se confronter à la réalité, notamment grâce au logiciel Belenios et aux interactions avec des entreprises. Nous avons agi en tant que tiers au cours des élections législatives de 2022 pour vérifier que tout s'était bien passé : ce travail nous a mis en contact avec l'Anssi et nous a permis de prendre conscience de nombreuses réalités de terrain.

Nous sommes informaticiens, spécialistes de sécurité informatique. Mais les sciences humaines ont aussi beaucoup à dire sur le vote électronique. Nous sommes sensibles à ces aspects, nous avons un avis, mais nous ne sommes experts ni en droit, ni en sciences sociales, ni en sciences politiques, ni en ergonomie. Nous ne pourrons donc pas répondre à toutes vos questions de façon aussi éclairée que le pourraient des spécialistes de ces disciplines.

Pour résumer nos conflits d'intérêts, ou en tout cas tout ce qui pourrait être interprété comme tel, je précise que nous avons interagi avec différentes entreprises dans le cadre de contrats de recherche que ces dernières – je pense notamment à Docaposte, Voxaly et Idemia, qui sont des entreprises françaises, ou encore à Scytl, qui est espagnole – avaient conclus avec le CNRS. Nous avons encore un contrat de recherche avec la poste suisse, qui vise le marché spécifiquement suisse du vote électronique.

Par ailleurs, le logiciel Belenios est en train d'être valorisé par l'ingénieur qui a développé le site, dans le cadre d'une start-up, mais nous-mêmes ne sommes pas impliqués ; nous ne détenons pas de part du capital.

M. Antoine Léaument, rapporteur. La question de la sécurité du vote électronique se pose de différentes façons.

Il y a d'abord la sécurité pour l'électeur lui-même : comment peut-il être sûr que son vote a bien été exprimé, et en faveur du candidat pour lequel il entendait voter ? Il pourrait craindre d'avoir voté pour un candidat, mais que la machine ait été "bidouillée" de telle façon qu'il aurait en fait voté pour un autre… Comment garantir la sécurité pour l'électeur ?

Comment garantir aussi que des intervenants extérieurs – des puissances étrangères ou un parti politique – ne puissent pas trafiquer le résultat du vote ?

Le vote en ligne a été proposé aux électeurs français inscrits à l'étranger aux élections législatives de 2012, de 2022 et de 2024, mais pas en 2017 : cette année-là, l'Anssi a estimé que les risques de cybersécurité étaient trop importants. Pourriez-vous nous en dire davantage ? Quels sont ces risques et comment s'en protéger ?

En 2022, ce vote électronique a rencontré des problèmes d'accès au serveur, qui ont empêché certains électeurs d'exprimer leur vote. Pouvez-vous nous expliquer ce qui s'est passé ?

Mme Véronique Cortier. Nous sommes dans le vif du sujet… Garantir à chaque électeur que son vote est compté est une question fondamentale, non résolue dans l'état de l'art. En effet, l'électeur choisit son candidat sur l'écran, mais il ne maîtrise pas ce qui est fait dans la machine. Des attaques peuvent survenir à au moins deux endroits : sur la machine de l'électeur – son ordinateur, son smartphone – et sur le serveur qui collecte les votes.

La vérifiabilité de l'intention reste une question très difficile : la personne choisit un nom qu'elle voit sur l'écran, mais sommes-nous certains que c'est bien ce nom qui est envoyé ? Certains pays arrivent à obtenir des garanties sur ce point, la Suisse ou l'Estonie par exemple. Ainsi, en Suisse, l'électeur reçoit à l'avance un matériel électoral qui comprend, pour chaque candidat, un code de quatre chiffres ; s'il sélectionne le candidat A, il y a un échange entre l'ordinateur du votant et le serveur et, en retour, l'électeur voit un code s'afficher, qui est normalement celui du candidat A. Or son ordinateur, même s'il est compromis, n'a pas accès à cette feuille de papier. Cela passe ainsi par une procédure papier, et l'infrastructure est lourde ; il faut plusieurs serveurs de vote. Il y a d'autres façons de procéder, mais disons pour faire court que si, sur le plan académique, nous savons vérifier les intentions, cela reste difficile à appliquer, soit parce que c'est cher, soit parce que l'on demande plus d'efforts à l'électeur. C'est vraiment une question à laquelle nous avons encore du mal à répondre.

Nous savons un petit peu mieux faire pour la suite du processus. Pour les élections législatives de 2022, on a supposé que l'ordinateur du votant était de confiance, qu'il chiffrait correctement le vote conformément au choix de l'électeur. C'était vraiment une hypothèse. À partir de là, on peut faire un peu plus : l'électeur obtient un récépissé – ce qui implique beaucoup de cryptographie –, à l'image d'un suivi de La Poste. On peut aussi s'assurer que le bulletin chiffré est bien dans l'urne et que le résultat proclamé correspond aux bulletins chiffrés. C'est le rôle que nous avons joué en tant que tiers de confiance. Pour cette seconde partie, l'état de l'art nous indique comment faire ; ce n'est pas toujours mis en œuvre dans la réalité.

Quant aux attaques éventuelles et aux craintes que l'on peut nourrir, tout dépend de l'élection considérée : l'élection de délégués de parents d'élèves dans un lycée n'a pas les mêmes enjeux qu'une élection nationale.

Les attaques peuvent aussi venir de l'intérieur : il y a forcément un humain pour gérer un serveur de vote. Le prestataire n'a *a priori* pas de raison de truquer l'élection, la commission électorale est *a priori* de bonne foi. Mais parmi tous ces intervenants, certains peuvent être corrompus – dette de jeu ou intérêt personnel, par exemple – et vouloir tenter d'enlever des bulletins, d'en rajouter, de manipuler le résultat. De la même façon, une puissance étrangère pourrait chercher à corrompre des employés d'un prestataire, par exemple. Dans le cas des élections législatives de 2022, le serveur était déployé par le ministère des affaires étrangères : là encore, il est possible que des puissances étrangères ou des attaquants internes cherchent à corrompre des personnes.

Quant à la corruption des dispositifs de l'électeur – ordinateur personnel ou smartphone –, elle sera probablement détectée à terme, mais une puissance étrangère pourrait chercher à déployer des virus sur certaines machines. Il n'est pas nécessaire de compromettre toutes les machines : il peut suffire d'agir sur un certain pourcentage du parc pour changer le résultat de l'élection. Bien sûr, tout dépend de l'enjeu, et donc de l'ampleur des moyens déployés.

M. Pierrick Gaudry. Je précise que nous employons le terme « corrompu » pour les machines comme pour les êtres humains, mais pas forcément à bon escient, car il est beaucoup plus négativement connoté dans ce second cas. Nous voulons seulement parler de quelqu'un qui se retrouve du côté de l'attaquant – mais un ingénieur système « corrompu » peut aussi bien être menacé, par exemple, ce qui n'est pas tout à fait la même chose.

En 2017, l'Anssi a en effet préconisé, quelques mois avant la tenue du scrutin, de ne pas autoriser le vote par internet pour les élections législatives dans les circonscriptions des Français de l'étranger. Nous ne savons pas ce qui s'est passé. L'analyse de risques qui mène à ce type de décisions est multiple. Elle s'attache d'abord au produit de vote lui-même – ses forces, ses faiblesses, ses failles éventuelles ; or, à cette époque, la réglementation n'obligeait pas à en rendre publiques les spécifications. Nous ne les connaissons donc pas. C'était le résultat d'un appel d'offres : nous connaissons l'entreprise qui l'a remporté, et d'autres circonstances où cette solution a été déployée. C'était un produit plutôt bon, leader européen à l'époque. Peut-être y a-t-il eu des soucis particuliers liés à cette élection. Mais l'analyse des risques prend aussi en considération un contexte géopolitique que nous ne sommes, en tant que chercheurs informaticiens, absolument pas aptes à évaluer.

L'Anssi est vraiment l'entité capable de prendre ce genre de décisions. Il faut admettre que, de temps en temps, des gens bien informés sont capables de dire qu'il ne faut pas utiliser le vote électronique : savoir renoncer est une qualité dans ce genre de situations.

L'Anssi communique beaucoup. Elle met ainsi régulièrement à jour un « panorama de la cybermenace » qui explicite l'environnement général et aide à comprendre pourquoi on préfère parfois renoncer.

À partir de 2022, la transparence sur le logiciel utilisé s'est accrue. Nous en savons donc davantage, d'autant que nous avons été impliqués en tant que tiers.

S’agissant des problèmes rencontrés en 2022 et en 2023 – pour les élections générales ou les partielles à la suite d’annulations, je ne saurais plus vous dire –, ils n’étaient pas spécifiques au vote électronique : c’était des serveurs qui n’étaient pas accessibles, des SMS qui n’arrivaient pas. Ce sont des difficultés que l’on pourrait avoir avec le serveur d’une banque ou un service des impôts. Des problèmes de sécurité informatique générale de ce type affectent particulièrement une procédure de vote électronique, soumise à des échéances courtes. En général, on peut se permettre que le serveur tombe pendant de courts moments, parce que la période de vote électronique est plus longue que pour le vote à l’urne : tenir physiquement un bureau de vote, dans une mairie ou une école, cela ne peut guère se faire plus qu’un dimanche de huit à vingt heures, alors qu’un système de vote par internet peut être ouvert durant plusieurs jours, ce qui permet de compenser d’éventuels problèmes d’accès. Mais si ceux-ci sont trop importants, il y aura un effet sur la participation.

M. le président Thomas Cazenave. Vous étiez tiers de confiance pour les élections législatives de 2022. Diriez-vous que, s’agissant du vote électronique, elles se sont bien déroulées ?

Vous expliquiez que l’état de l’art donne des moyens d’assurer une vérifiabilité parfaite, mais que ce n’est pas tout à fait le cas des systèmes effectivement mis en place. Ai-je bien résumé votre propos ? Considérez-vous que le vote à l’urne est absolument sans risque par rapport à un vote électronique ?

Vous relevez dans votre ouvrage que les pays ayant instauré le vote par internet ne constatent pas d’augmentation de la participation électorale. Dès lors, pourquoi avoir recours à cette modalité de vote susceptible de présenter des fragilités, des risques de vulnérabilité et de « non-vérifiabilité » ? À quoi bon ? Pourriez-vous revenir sur ce que vous avez observé et sur les échanges que vous avez peut-être eus avec vos collègues qui, dans d’autres pays, sont spécialistes de ces sujets ?

Je termine par une question de béotien : les enjeux de vérifiabilité et de non-vulnérabilité sont-ils les mêmes pour une machine à voter dans un bureau de vote et pour le vote à distance par internet ? Autrement dit, ces deux modalités présentent-elles les mêmes risques ? S’il s’avère que, dans l’isoloir d’un bureau de vote, les machines à voter posent plus de problèmes que les bulletins papier, à quoi bon les utiliser ?

Mme Véronique Cortier. Ces questions, que nous nous posons régulièrement, sont très importantes.

Nous n’avons pas participé à la supervision du vote en ligne lors des élections législatives de 2024. Tout s’est-il bien passé en 2022 et 2023 ? En tant que scientifiques, il nous est difficile d’apporter une réponse définitive à cette question.

Vous avez vous-même évoqué les problèmes d’accessibilité rencontrés en 2022. Sur les onze circonscriptions, trois élections ont dû être réorganisées en 2023, dont au moins deux parce qu’un nombre très significatif d’électeurs n’avaient jamais reçu par SMS les codes dont ils avaient besoin – je me réfère aux décisions rendues par le Conseil constitutionnel, car je n’ai pas plus d’informations. Il est donc difficile de voir dans ces opérations de vote un succès total.

Le système mis en œuvre résulte d’un compromis, car toutes les possibilités existantes en l’état de l’art n’ont pas été retenues. Notre rôle consistait à vérifier que les résultats proclamés correspondaient aux bulletins déposés dans l’urne qui nous avait été fournie et que les électeurs

ont pu retrouver le numéro inscrit sur leur récépissé dans la liste des références de bulletins publiée. Sur ces questions, nous n'avons pas constaté de dysfonctionnement. Cependant, nous n'avons observé qu'une petite partie du processus.

Il ne faut pas oublier que ce vote électronique remplace le vote par correspondance autrefois proposé aux Français de l'étranger qui ne peuvent pas se déplacer jusqu'à un bureau de vote physique ou ne sont pas disposés à faire la queue. Ce vote par correspondance était un vote papier, mais à distance. Il convient de dépasser la distinction classique entre le vote électronique et le vote papier. Si le vote papier à l'urne, tel qu'il est organisé en France pour les grandes élections, garantit un très bon niveau de sécurité, l'utilisation de bulletins papier ne suffit pas pour assurer la fiabilité du système. En France, la sécurité du vote par correspondance n'est pas exceptionnelle : les votants ne sont même pas assurés que leur bulletin arrive à destination, parce que les services postaux peuvent dysfonctionner ou délivrer les plis en retard ; par ailleurs, ils ne savent pas qui réceptionne les bulletins et n'ont pas la garantie que le secret du vote soit respecté, ni que les personnes chargées de collecter les bulletins ne prennent pas l'initiative de les changer. Dès lors, le vote électronique n'apparaît pas pire que le vote par correspondance ; on peut même concevoir des systèmes de vote électronique garantissant plus de sécurité tout en répondant aux besoins des personnes empêchées de se déplacer.

On peut ainsi considérer que le recours au vote électronique était satisfaisant pour l'élection des députés des Français de l'étranger. Cela ne veut pas dire qu'il aurait été opportun d'utiliser ce même système sur le territoire national, où les électeurs ont la possibilité de se déplacer pour voter physiquement.

Je confirme que le système mis en place n'utilisait pas toutes les possibilités existantes en l'état de l'art. Je l'ai dit, il résulte d'un compromis et de nos discussions avec l'Anssi, qui va rédiger un guide et des recommandations. En tant que chercheurs, nous encourageons le recours à certaines techniques qui nous semblent accessibles, mais il revient aux autorités de décider de ce qui est faisable sans être trop coûteux.

Vous nous avez demandé si le vote à l'urne était à 100 % sans risque. En tant qu'informaticiens spécialistes des questions de sécurité, nous considérons qu'il existe toujours des risques ! Cependant, le vote à l'urne, tel qu'il est pratiqué en France, comporte deux avantages.

Le premier est la simplicité : l'électeur choisit le plus souvent un candidat ou une liste parmi une dizaine voire une vingtaine, et l'on compte simplement le nombre de voix recueillies par chacun. Cela n'a rien à voir avec ce qui se passe dans d'autres pays où il faut classer les candidats ou répondre à de nombreuses questions en même temps ; ces règles électorales difficiles à mémoriser multiplient les risques d'erreur et conduisent à rendre un grand nombre de bulletins invalides. En France, il suffit donc de compter, ce qui peut être un peu long mais reste tout à fait faisable. Les systèmes plus compliqués peuvent encourager le recours au vote électronique ; du reste, quand le comptage est très difficile ou quand les électeurs doivent classer les différents candidats, il est nécessaire d'utiliser un ordinateur pour déterminer le vainqueur.

Le vote à l'urne apparaît donc très sûr : l'électeur voit les bulletins ; il se rend dans l'isoloir pour glisser celui qu'il choisit dans une enveloppe, afin de protéger son secret ; il dépose lui-même cette enveloppe dans l'urne ; il peut rester au bureau de vote toute la journée ou faire confiance à ceux qui restent sur place pour vérifier que personne ne manipule l'urne. Certaines fraudes demeurent possibles – je pense par exemple aux faux électeurs – mais sont

pratiquées à petite échelle. Ainsi, le système n'est pas sûr à 100 %, mais tout de même très sûr par rapport aux autres.

Le second avantage du vote à l'urne, en France, est son caractère compréhensible : les électeurs peuvent comprendre, sur-le-champ ou avec un peu de recul, pourquoi il est sécurisé. Par exemple, s'il est interdit d'écrire sur son bulletin, c'est pour éviter que l'on soit forcé d'y porter un signe distinctif qui permettrait de le reconnaître. On suit les règles sans forcément savoir pourquoi, mais elles sont simples et connues.

Ainsi, de notre point de vue, aucun système de vote électronique n'est aussi sûr que le vote à l'urne, en présentiel, tel qu'il est organisé en France pour les grandes élections. Dès lors, nous ne voyons aucune raison de changer de système. À quoi bon passer au vote électronique ? Nous nous posons régulièrement la question.

Les machines à voter ne réduisent pas les contraintes par rapport au vote à l'urne : les électeurs doivent toujours se déplacer. Du reste, ce système est moins compréhensible, et il est exposé à plus de vecteurs d'attaque. Les machines peuvent être compromises, surtout si elles font l'objet d'un moratoire depuis plusieurs années – généralement, la première chose à faire pour garantir la sécurité d'un appareil, c'est de le mettre à jour… Vraiment, nous ne voyons aucune raison d'utiliser des machines à voter en France. Il est vrai que, dans certains pays, elles sont indispensables pour compter les votes. Ainsi, les États-Unis utilisent des machines mécanisées, à levier, depuis plus d'un siècle, parce que les électeurs répondent à de nombreuses questions à la fois : ils choisissent le gouverneur de l'État en même temps que l'heure d'arrosage des pelouses – j'exagère peut-être un peu. Sans ces machines, le comptage serait difficile, long et pénible. En France, cette étape allonge le processus de quelques heures, mais elle est tout à fait réalisable avec de simples moyens humains. Dans le contexte français, on ne voit pas quel serait l'avantage des machines à voter.

M. Pierrick Gaudry. On pourrait croire que le vote par internet, en permettant aux électeurs de voter depuis n'importe quel endroit, entraîne forcément une augmentation de la participation. C'est un raccourci. Nous touchons là à des questions sociologiques dont nous ne sommes pas spécialistes – nous nous contentons d'observer –, mais si les pays ayant mis en œuvre cette nouvelle modalité de vote ont pu connaître, au début, un petit pic de participation, sous l'effet de la nouveauté, le taux de participation s'est ensuite rapidement stabilisé. Cette tendance semble toucher assez uniformément tous les pays concernés. Je prendrai l'exemple de l'Estonie, qui autorise le vote par internet depuis 2007. Il s'agit d'un régime parlementaire, qui ne connaît pas d'élection présidentielle : pour eux, les élections législatives, c'est le top…

M. le président Thomas Cazenave. Je suis obligé de corriger vos propos, monsieur Gaudry : pour nous aussi, les élections législatives, c'est le top !

M. Pierrick Gaudry. Bien sûr, monsieur le président !

En Estonie, donc, lors des dernières élections législatives, plus de la moitié des votants ont utilisé internet, mais le taux de participation s'est limité à 63,5 %. Ce taux est très comparable à ceux que nous connaissons en France, même s'ils varient en fonction du contexte. Je ne pense donc pas que le vote électronique nous permette de retrouver les taux de participation que nous avons connus dans la période d'après-guerre. Ce n'est pas une solution pour limiter l'abstention.

Le vote par internet permettrait-il d'alléger le dispositif de tenue des bureaux de vote, qui est très lourd et requiert la présence de nombreux assesseurs ? Il est vrai qu'un passage au tout-électronique diminuerait les besoins humains le jour J. Cependant, tous les pays ayant mis en place un vote par internet pour leurs élections politiques majeures ont gardé un système multimodal, où le vote à l'urne reste possible. Il faudra donc, de toute façon, maintenir des bureaux de vote. Peut-être pourrait-on en supprimer 30 %, mais la question de la proximité se poserait immanquablement. On ne voit donc pas bien quel sera le gain…

Pour les élections présidentielles, législatives et municipales, notre point de vue est assez clair : nous ne voyons pas l'intérêt de passer au vote par internet. Les risques associés à cette modalité de vote ne compensent pas les gains mineurs pour ce qui est de l'abstention ou des besoins dans les bureaux de vote. Le jeu n'en vaut pas la chandelle.

M. le président Thomas Cazenave. Merci pour la clarté de vos propos. Si je comprends et résume bien, vous estimez que le vote électronique est intéressant, y compris du point de vue de la sécurité, lorsqu'il se substitue au vote par correspondance, mais dans les autres cas de figure, vous n'y voyez pas d'intérêt.

Mme Véronique Cortier. C'est un bon résumé de notre position, du moins pour les élections nationales ou pour les élections citoyennes à enjeu, car le vote à l'urne présente bien plus d'avantages du point de vue de la sécurité.

Il conviendrait peut-être de tempérer un peu notre point de vue s'agissant d'autres scrutins tels que les élections professionnelles, dont les enjeux peuvent d'ailleurs ne pas être négligeables. L'organisation d'un vote à l'urne n'est pas forcément simple ; du reste, les urnes sont parfois déplacées avant le dépouillement, ce qui pose des problèmes de sécurité. Dans certains contextes, le vote électronique peut donc avoir un intérêt.

M. Antoine Léaument, rapporteur. Je vous remercie de votre franchise : alors que vous êtes chercheurs dans ce domaine, vous dites que le vote électronique ne présente finalement pas beaucoup d'intérêt. Bien que vous ayez présenté tout à l'heure tous les risques de conflits d'intérêts auxquels vous pourriez être confrontés, je n'ai aucun doute quant à votre sincérité !

Le vote à l'urne n'a pas qu'une dimension individuelle. Il s'inscrit dans un cadre collectif, organisé et ritualisé, qui implique la participation de nombreuses personnes : l'électeur rencontre d'abord des gens qui vérifient son inscription sur les listes électorales ; il se rend ensuite dans l'isoloir pour glisser son bulletin dans une enveloppe ; devant l'urne, un nouveau cérémonial commence, car il faut vérifier une nouvelle fois que l'électeur est bien inscrit avant qu'il puisse déposer son enveloppe. Il y a donc une forme de contrôle collectif, auquel participent notamment les partis politiques, qui peuvent nommer des assesseurs chargés de vérifier le bon déroulement du scrutin.

Les choses semblent plus compliquées, ou en tout cas plus techniques, en cas de scrutin électronique. Comment les assesseurs représentant les partis politiques pourraient-ils remplir leur rôle dans un tel cadre ? Comment pourraient-ils notamment contrôler le dépouillement, en dépit de son caractère instantané, et attester de la fiabilité du scrutin ? Faudrait-il que chaque parti recoure à des informaticiens ?

S'agissant des machines à voter, je suis assez d'accord avec ce que vous avez dit. Puisque le vote à l'urne fonctionne bien, pourquoi se compliquer la vie avec des outils qui

viendraient par ailleurs ajouter de la suspicion ? Je vois quand même un avantage potentiel à ces machines : si elles étaient connectées au répertoire électoral unique, elles pourraient permettre à tout électeur de voter où qu'il se trouve, même à l'autre bout de la France – la machine se chargerait de trouver dans quel bureau de quelle commune il est inscrit. Un tel système est-il envisageable, sur les plans théorique et pratique ? Si oui, quels en seraient les risques ?

On a beaucoup parlé de ce que vous appelez la « vérifiabilité », c'est-à-dire de la possibilité de vérifier que l'électeur a bien voulu faire ce qu'il a fait. Or, on l'a dit, le vote à l'urne se caractérise par une forme d'organisation collective, de rituel : lorsqu'un électeur se présente dans un bureau de vote, on peut constater qu'il n'est influencé par personne et que, même s'il est accompagné par quelqu'un qui le surveille, il se rend seul dans l'isoloir avant de déposer dans l'urne le bulletin de son choix. Même s'il y a des pressions, elles ne peuvent pas s'exercer jusqu'au bout. Tel n'est pas le cas pour le vote à distance : nous n'avons aucun moyen de vérifier que des électeurs particulièrement fragiles, notamment des personnes en situation de dépendance, ne votent pas sous la pression de quelqu'un d'autre.

Il apparaît que le vote électronique est beaucoup plus utilisé pour des élections non nationales et non citoyennes, telles que les élections des délégués du personnel. Une forme de confiance s'est-elle instaurée ? Avez-vous eu des retours s'agissant de l'efficacité du vote électronique dans ce contexte ? On sait par exemple que les élections des délégués du personnel se caractérisent par une participation très faible : le vote électronique a-t-il permis de l'augmenter ?

L'exemple de l'Estonie, que vous avez cité, est très intéressant, car ce pays est l'un des plus avancés en matière de vote électronique. Certes, le taux de participation aux dernières élections n'est que de 63 %, mais qui a voté ? En France, l'abstention est socialement située : les plus jeunes votent moins, les plus âgés votent davantage. On pourrait supposer que le vote électronique permet de corriger cet écart, compte tenu de la fracture numérique qui éloigne les plus anciens de l'utilisation des outils informatiques, tandis que les jeunes sont de grands utilisateurs des nouvelles technologies. Constate-t-on une telle correction dans les pays où cette nouvelle modalité de vote a été introduite ?

Mme Véronique Cortier. Pour assurer le contrôle collectif du scrutin, il faut commencer par rendre le système ouvert, autrement dit par rendre publiques les spécifications, la description du système. Cela revient, dans une certaine mesure, à déléguer à la communauté des geeks, des informaticiens, des programmeurs, des acteurs du monde académique le soin de vérifier que le système assure les bonnes propriétés. C'est quelque chose qui se fait de manière naturelle dans le monde de la sécurité. Le bon fonctionnement du protocole sécurisé que l'on utilise sur internet – les adresses qui commencent par https – repose sur son caractère public : de nombreuses personnes regardent la chose de près, essaient de trouver des failles dans le dispositif, de les corriger, etc. C'est la première étape à suivre pour avoir un système de vote correct.

Il peut être difficile pour les partis politiques de vérifier que le système fonctionne correctement mais des citoyens s'y emploieront. En Suisse, cette participation est encouragée au moyen de *bug bounties* – ou primes aux bogues –, dont le montant peut atteindre 150 000 euros pour l'objectif le plus difficile : modifier le résultat sans être détecté. Cela permet de faire progresser le système et de vérifier qu'il assure le niveau de propriétés souhaité eu égard aux menaces identifiées.

La Suisse est un exemple intéressant car c'est un des pays qui a le niveau d'exigence le plus élevé en matière de vote électronique. Les Suisses exposent de façon très claire et très précise les propriétés qu'ils demandent ainsi que les personnes à qui ils font confiance et ne font pas confiance. La Poste y est, par exemple, réputée de confiance : on part du principe que le matériel envoyé aux électeurs ne fera pas l'objet de manipulations. C'est important pour l'informaticien, à qui il n'appartient pas de décider à quel dispositif il est raisonnable de faire confiance pour telle ou telle élection. L'appréciation, en la matière, dépend des menaces analysées par des organismes tels que l'Anssi, mais aussi de choix politiques, citoyens.

Une fois que l'on a un système auquel on fait à peu près confiance, on fait intervenir des assesseurs virtuels. Lors des législatives de 2022, nous avons assumé ce rôle. On nous a donné une urne chiffrée, qui correspond aux bulletins placés dans leur enveloppe. De la même manière que l'on sait chiffrer ou signer, on est en mesure de démontrer que le résultat de l'élection – tel qu'il apparaît en ligne – correspond aux bulletins chiffrés : on fait appel, pour ce faire, à des preuves cryptographiques nommées « preuves à divulgation nulle de connaissance ». Au moment où l'on déchiffre, on peut prouver qu'on effectue correctement l'opération. Nous avons réalisé l'ensemble des tâches, de bout en bout : nous avons pris le temps de comprendre comment le système fonctionnait, nous avons écrit le code permettant d'opérer les vérifications et nous l'avons exécuté sur l'urne.

Si le système est public, un parti politique peut, lui aussi, écrire son propre code informatique. Mais, si du code de référence est publié et qu'un nombre suffisant de personnes s'est assuré que le code est correct et permet de vérifier la correspondance entre le résultat et les bulletins, les partis politiques n'ont pas nécessairement besoin de tout réécrire : ils peuvent se contenter d'exécuter un logiciel existant et de procéder aux vérifications.

Il n'est peut-être pas indispensable que chaque parti se dote d'un informaticien mais il faut tout de même une montée en compétence.

M. Pierrick Gaudry. La transparence sur le système utilisé est essentielle : c'est un prérequis qui offre la possibilité aux citoyens comme aux partis politiques de vérifier que les choses se sont bien passées. Le fait que tout le monde ne soit pas informaticien n'est pas une excuse pour ne pas rendre ces informations transparentes, car on peut déléguer la vérification à des personnes de son choix – professionnels ou non. On peut faire une analogie avec la loi : celle-ci est compliquée si je vais la consulter sur Legifrance mais je sais que je peux faire appel à un conseil de mon choix qui va m'aider à la comprendre, car elle est transparente.

Mme Véronique Cortier. Vous demandiez si l'utilisation de machines à voter permettrait de voter dans n'importe quel bureau de vote. Je ne vois pas ce qui l'empêcherait. Il faudrait sans doute prévoir une authentification plus forte pour s'assurer qu'il s'agit de la bonne personne.

Toutefois, les machines à voter utilisées en France ne disposent d'aucun mécanisme de vérifiabilité : il faut donc avoir confiance en elles. Certains de nos collègues, dans le milieu académique américain, ont pour spécialité d'attaquer ce type de machines : ils installent des programmes tels que Pac-Man pour montrer que l'on peut y implanter absolument n'importe quoi. En outre, ces machines sont stockées pendant des mois, voire des années, dans un hangar. Peut-on être certain que personne ne s'y introduira, qu'une puissance étrangère ne sera pas en mesure d'installer de petits dispositifs sur les machines afin de changer le résultat, le jour J ?

Aux États-Unis, on ajoute de la vérifiabilité sur les machines : après avoir sélectionné, sur l'écran, le candidat pour lequel il souhaite voter, l'électeur peut voir le bulletin imprimé, ce qui lui permet de vérifier que son intention a été respectée. Il confirme alors son vote et le bulletin tombe dans une urne. Par la suite, on comptabilise les bulletins déposés dans un certain nombre d'urnes pour vérifier que le total de ces bulletins correspond au résultat. On renforce la vérifiabilité en ajoutant du papier – mais cela ne fonctionne pas dans votre hypothèse, celle où on se déplace, car le papier ne peut aller dans une autre urne.

La question est de savoir si l'on veut faire complètement confiance à des machines de vote pour des scrutins à fort enjeu.

M. Pierrick Gaudry. Pour que l'on puisse voter dans n'importe quel bureau, il faudrait probablement que les machines soient connectées au réseau, afin de s'assurer qu'une même personne ne vote pas en deux lieux différents. Or, pour sécuriser une machine à voter, on commence par couper toutes ses interfaces. Le fait de connecter la machine augmenterait la surface d'attaque. C'est une des raisons pour lesquelles, très probablement, cela ne se fera pas dans l'immédiat.

Mme Véronique Cortier. Comment s'assurer de la pleine liberté d'expression du vote ? C'est une question essentielle dans le cadre du vote électronique, à laquelle on ne sait répondre qu'imparfaitement. Notre logiciel Belenios permet de voter une deuxième fois, par exemple quelques heures après le premier vote. Naturellement, seul le dernier vote sera pris en compte. Cela permet de changer d'avis – ce qui peut être discuté – mais aussi de modifier son vote si l'on ne s'est pas senti libre la première fois – par exemple, si un membre de votre famille vous a aidé, ou si vous avez voté collectivement, avec vos collègues, pour élire les représentants du personnel. Cette technique offre une certaine protection contre des attaquants disposant de moyens faibles, qui ne vérifieront pas que le vote a changé, soit parce qu'ils n'en ont pas la volonté, soit parce qu'ils n'en sont pas capables techniquement. On peut toutefois faire face à des attaquants qui se livrent à des pratiques mafieuses telles que l'achat de votes. Or il est très difficile de concevoir des systèmes résistant à la coercition.

De surcroît, il existe des aspects psychologiques auxquelles les solutions techniques ne suffisent pas à répondre. Si l'on propose un système sûr, les gens voteront-ils, malgré la pression, pour le candidat de leur choix ? C'est discutable. Et, quoi qu'il en soit, les réponses techniques, telles que la réalisation de faux matériels de vote, sont très difficiles à mettre en œuvre.

J'en viens aux élections dites non citoyennes, qui présentent des enjeux variables : ceux-ci sont assez faibles pour une élection comme celle des représentants des parents d'élèves au conseil de classe, mais peuvent être plus importants pour les élections professionnelles. Les primaires politiques, quant à elles, peuvent être porteuses d'un fort enjeu ; des puissances étrangères pourraient souhaiter interférer dans leur bon déroulement. Pourtant, en ce qui les concerne, seules les recommandations de la Commission nationale de l'informatique et des libertés (Cnil) s'appliquent.

Le vote électronique est très utilisé dans le cadre des élections des représentants du personnel. Il me semble même qu'un décret le rend obligatoire, pour certains scrutins, dans la fonction publique. À notre connaissance, il n'a pas d'influence sur la participation – nous l'avons d'ailleurs constaté à notre modeste échelle, sur la plateforme Belenios, pour de petites élections sans grand enjeu.

M. Pierrick Gaudry. Je n’ai pas d’information sur l’effet du vote électronique sur la participation selon l’âge des électeurs. Cela étant, des conclusions qui paraissent évidentes peuvent se révéler erronées. Un chercheur en sciences sociales a montré que, contrairement à ce que l’on pourrait croire, les personnes âgées commettent moins d’erreurs dans le parcours de vote que les jeunes : en effet, ces derniers ont tendance à cliquer un peu partout jusqu’à ce que ça marche, tandis que les plus âgés suivent la documentation pas à pas.

M. le président Thomas Cazenave. Vous expliquez très clairement que le vote électronique est utile pour remplacer des procédures défaillantes ou très risquées. Or, parmi les modalités de l’acte de vote, il en est une qui ne fonctionne pas très bien, compte tenu du coût que représente la démarche : je veux parler du vote par procuration. Avez-vous cherché à améliorer le dispositif employé pour ce vote ? Les solutions techniques sur lesquelles vous avez travaillé offrent-elles des moyens simples pour fluidifier le processus, notamment en limitant les étapes nécessaires à la validation des procurations ?

Mme Véronique Cortier. C’est un problème très peu étudié sur le plan académique. Je n’ai pas de réponse précise à vous apporter. Cela touche à l’authentification, qui est un problème difficile dans le cadre du vote électronique. En France, généralement, un matériel spécifique est fourni pour chaque élection : on reçoit par courrier, par mail ou par SMS des identifiants et un mot de passe pour voter. C’est une authentification très faible dans la mesure où une personne qui intercepte le message peut se substituer à l’électeur. Ce dernier peut aussi donner ses identifiants – ce qui est une forme de procuration non officielle –, les vendre ou les perdre.

En Estonie, une carte d’identité nationale permet un meilleur niveau d’authentification, car elle contient une puce nécessaire au vote. On pourrait probablement simplifier le système de procuration grâce au vote électronique si l’on disposait d’une authentification plus forte, telle que celle existant en Estonie. D’un point de vue pratique, actuellement, on peut seulement donner ses identifiants, mais, en agissant de la sorte, on empêche les autorités de contrôler qu’une même personne n’a pas reçu plus d’une ou deux procurations. Pour donner procuration officiellement, il faut accomplir une démarche particulière, qui n’est pas vraiment faisable en ligne. Pour l’instant, on ne peut pas s’authentifier de manière fluide, mais on peut imaginer que des progrès auront lieu au cours des prochaines années.

M. Pierre-Yves Cadalen (LFI-NFP). Étant député de Brest, j’ai été élu, pour les deux tiers de la circonscription, par des votes effectués sur des machines à voter, lesquelles viennent des Pays-Bas. Je lisais ce matin une étude de l’universitaire Rop Gonggrijp, qui met en doute la fiabilité de ces machines. Cela a conduit les Pays-Bas, en 2009, à retirer l’ensemble des machines, de marque Nedap, qui demeurent pourtant agréées par le ministère de l’intérieur français. La même année, la Cour constitutionnelle allemande a décidé le retrait de l’ensemble des machines à voter en raison de l’absence de vérifiabilité des résultats. Dans notre pays, pourtant, environ 1 million d’électrices et d’électeurs votent de cette façon. Pourquoi la France ne prend-elle pas des mesures similaires à celles qui ont été décidées aux Pays-Bas et en Allemagne, alors qu’elle fait face aux mêmes problèmes et qu’aucune contre-expertise n’a été réalisée ?

Mme Véronique Cortier. Nous ne le savons pas. Nous avons lu les mêmes études que vous. Je le disais, des collègues américains ont mené des attaques contre des machines à voter. La vérifiabilité de ces machines n’a fait l’objet d’aucune amélioration, ce qui s’explique aussi par le fait qu’en France, un moratoire a été décidé. Nous nous demandons également

pourquoi elles sont encore utilisées dans notre pays – leur niveau de sécurité étant reconnu comme peu satisfaisant – et à quels problèmes cela répond.

M. Pierrick Gaudry. Peut-être les communes souhaitaient-elles amortir leurs investissements. Cela étant, nous sommes en 2025 : il faudrait se demander quel levier on peut actionner pour que le moratoire se transforme en interdiction. En tout état de cause, cela nous semble une mauvaise idée de continuer à les utiliser.

M. le président Thomas Cazenave. Nous vous remercions pour les éclairages précieux, parfois contre-intuitifs, que vous nous avez apportés.

La séance s’achève à dix heures cinquante-cinq.

Membres présents ou excusés

Présents. - M. Pierre-Yves Cadalen, M. Thomas Cazenave, Mme Nicole Dubré-Chirat, M. Antoine Léaument.