Strasbourg, le 20 novembre 2019

CDDG(2019)7
Point 7.2 de l'ordre du jour

COMITE EUROPEEN SUR LA DEMOCRATIE ET LA GOUVERNANCE (CDDG)

LES NOUVELLES TECHNOLOGIES DANS LE CYCLE ELECTORAL. RECOMMANDATIONS DU CONSEIL DE L'EUROPE ?

Ardita Driza Maurer
Juriste, consultante indépendante, Suisse
septembre 2019

Pour information

Rapport d'expert
établi pour la
Direction générale de la démocratie
Service de la gouvernance démocratique

Table des matières

DÉFINITIONS ET DÉMARCHE

Cycle électoral

Du point de vue de l'organe d'administration des élections (OAE), un cycle électoral englobe toutes les étapes et tous les processus qui relèvent du périmètre des fonctions, responsabilités et pouvoirs de l'OAE et qui sont nécessaires au bon déroulement d'une élection ou d'un vote. De plus, la notion de cycle suppose que le processus soit réitéré élection après élection.

Les principales composantes du cycle électoral sont la conception et la rédaction de la législation, le recrutement et la formation du personnel électoral, la planification de l'élection, l'inscription des électeurs, l'inscription des partis politiques, la désignation des partis et des candidats, la campagne électorale, le scrutin, le dépouillement des bulletins de vote, le décompte des voix et la publication des résultats, la résolution des contentieux électoraux, la communication des informations, l'audit et l'archivage.

Le déroulement des votes de démocratie directe comprend les mêmes étapes, auxquelles s'ajoutent, entre autres, l'approbation formelle et/ou matérielle de la proposition (initiative ou référendum), le contrôle de la fiche servant à recueillir les signatures des personnes soutenant la proposition, la réception et le contrôle de validité des signatures, le décompte, la validation et la publication des résultats, et enfin l'organisation du vote si le nombre requis de signatures valides est atteint. Ensuite, comme dans le cas des élections, l'OAE informe les électeurs, procède à la planification et conduit le vote[1].

Dans le présent document, l'expression « élection/cycle électoral » désigne aussi bien les élections que les votes de démocratie directe.

Nouvelles technologies

Les technologies numériques connaissent une évolution rapide. L'expression « nouvelles technologies » désigne les technologies numériques qui ont été introduites le plus récemment dans le cycle électoral. Il s'agissait hier de la numérisation des documents/procédures et de la biométrie. Aujourd'hui, le terme « nouvelles » renvoie souvent aux chaînes de blocs, à l'informatique en nuage, à l'internet des objets ou à l'intelligence artificielle.

Méthode

Les nouvelles technologies utilisées dans le cycle électoral doivent respecter le droit à des élections libres (article 3 du Protocole n° 1 à la Convention européenne des droits de l'homme [CEDH]) ainsi que d'autres droits comme la liberté d'expression et la non-discrimination. Le présent document porte essentiellement sur l'article 3 du Protocole n° 1 à la CEDH. Garant des valeurs consacrées par la CEDH et ses Protocoles, le Conseil de l'Europe a pour mission essentielle de contrôler la mise en œuvre de la Convention dans et par les pays de la région. Cela vaut également pour les activités liées à des élections.

En vertu de l'article 3 du Protocole n° 1 à la CEDH et de la jurisprudence de la Cour européenne des droits de l'homme, l'OAE (c'est-à-dire l'État) a l'obligation positive de s'assurer que toutes les activités d'un cycle électoral, y compris celles qui s'appuient sur les technologies numériques, sont en conformité avec le droit à des élections libres.

[1] IDEA, *Electoral Management Design*, 2014, p. 12, 16 et 75 à 77.

À l'évidence, les nouvelles technologies améliorent et facilitent certains aspects des élections. Cela étant, l'évolution rapide de ces technologies, leur complexité et la connaissance limitée qu'on en a (en particulier la connaissance multidisciplinaire), leur imprévisibilité et même les attaques contre les processus électoraux (qui sont apparues avec ces technologies) fragilisent les OAE. Par ailleurs, ceux-ci subissent des pressions sociales et politiques qui les poussent à se moderniser tout en garantissant une sécurité globale.

C'est dans ce contexte qu'il convient d'examiner la question suivante : « Avons-nous besoin de recommandations de la part du Conseil de l'Europe sur l'utilisation des nouvelles technologies au cours des élections ? ». Par souci de concision, nous nous proposons de procéder comme suit : tout d'abord, nous passons en revue les caractéristiques de certaines nouvelles technologies, leurs usages et les problèmes qu'elles posent. Ensuite, nous examinons les différentes phases du cycle électoral afin de déterminer les nouvelles technologies/solutions utilisées ou envisagées et les problèmes de conformité qui se posent ou pourraient se poser. Enfin, nous proposons quelques scénarios en nous plaçant dans l'hypothèse où le Conseil de l'Europe proposerait des recommandations et nous examinons aussi les conséquences qu'aurait un choix inverse.

Il est à noter que la protection des élections contre les manipulations d'opinions (fausses informations, algorithmes [Facebook], etc.) n'entre pas dans le cadre du présent document, car cette question est traitée dans d'autres forums, au Conseil de l'Europe ou dans d'autres organisations[2].

UTILISATION DES NOUVELLES TECHNOLOGIES : AVANTAGES ET INCONVÉNIENTS

D'un point de vue technique

Numérisation

La numérisation désigne la conversion de textes, d'images ou de sons dans un format numérique pouvant être traité par un ordinateur. Cette technique est à la base de toutes les nouvelles technologies. Son principal avantage est de permettre le traitement — exempt d'erreurs, efficace, rapide, etc. — par ordinateur des informations numérisées.

Dans les pays du Conseil de l'Europe, la plupart des documents utilisés dans le cycle électoral sont numérisés : registres, bases de données, etc. La numérisation des processus est plus difficile, en particulier lorsqu'ils sont exécutés sur internet. Parmi les processus électoraux numérisés, on peut citer l'enregistrement électronique, l'identification électronique des électeurs (liste électorale électronique), le vote électronique (sur des machines à voter installées dans des bureaux de vote et sur internet), le dépouillement électronique et la transmission électronique des résultats (des bureaux de vote vers un système central par exemple).

[2] Voir par exemple Commission de Venise, *projet de Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité de la Direction Générale droits de l'homme et État de droit*, 7 juin 2019, CDL(2019)002.

À quoi doit ressembler un processus numérisé ? Cette question pose un dilemme qui doit être tranché : le processus doit-il imiter la manière de procéder « traditionnelle » (comme c'est le cas de la plupart des solutions à l'heure actuelle) ou peut-il prendre une forme totalement nouvelle, qui tire avantage des possibilités offertes par les nouvelles technologies ? Jusqu'ici, c'est l'imitation qui a primé. Ainsi, sous l'angle du « suffrage égal », un canal de vote électronique ne doit pas proposer de possibilités supplémentaires ou différentes par rapport à celles que propose un canal traditionnel. Cela étant, la logique utilisée est différente : elle n'est pas centrée sur des processus, mais sur des principes à protéger. Par exemple, le vote électronique étant exposé à des risques particuliers, le principe de vérifiabilité est introduit pour garantir le respect du principe de « suffrage libre et secret ». La vérifiabilité permet à l'électeur de vérifier son propre vote ainsi que le résultat général, ce qui constitue un nouveau processus, qui est en rupture par rapport aux processus traditionnels.

Biométrie

La biométrie offre la possibilité de saisir et de sauvegarder au format électronique certaines caractéristiques physiques (iris, empreinte digitale, image faciale, etc.) qui permettent d'identifier une personne de façon unique. Cette technique a été introduite dans l'espoir de garantir, entre autres, l'identification unique des électeurs et d'éviter les votes multiples, en particulier dans les pays où les registres traditionnels n'existent pas ou sont moins fiables qu'ailleurs.

Dans le cadre des élections, la biométrie (identification unique des électeurs par saisie des caractéristiques physiques biométriques et comparaison avec des données stockées dans des bases) est essentiellement utilisée hors d'Europe (Amérique du Sud, Afrique, etc.). Les principales préoccupations et raisons qui expliquent le refus de l'enregistrement biométrique des électeurs en Europe concernent la confidentialité des électeurs, la privation du droit de vote et la protection des données.

Chaînes de blocs

Une chaîne de blocs est une série d'enregistrements de données horodatés et immuables qui est distribuée et gérée par une grappe d'ordinateurs. Elle a pour principales caractéristiques la décentralisation, la transparence et l'immutabilité[3]. Les transactions étant enregistrées sur de nombreux ordinateurs, aucun enregistrement contenant une transaction donnée ne peut être modifié rétroactivement sans modification de tous les blocs ultérieurs.

Quelques expériences de vote mettant en œuvre la technique des chaînes de blocs ont été réalisées au niveau local[4]. Le vote par chaînes de blocs se prévaut de nombreux avantages par rapport aux systèmes de vote traditionnels, centralisés et sur support papier. Cela étant, la plupart des propriétés (identification électronique, signatures électroniques visant à garantir l'intégrité des données, cryptographie forte, vérifiabilité des électeurs, multiples possibilités de vote) ne sont pas l'apanage des chaînes de blocs, mais existent déjà dans le système de vote électronique vérifiable « traditionnel ». Le vote par chaînes de blocs introduit au moins une caractéristique nouvelle et en rupture avec ce qui se fait habituellement : toute information traitée, via un processus informatique ou de stockage de données, est distribuée sur de multiples nœuds (décentralisation). Dans un système de vote décentralisé, un ensemble d'entités doivent approuver la manière dont un suffrage a été exprimé avant qu'il soit enregistré. Autrement dit, aucune entité unique n'a le contrôle : le vote n'est pas validé uniquement par l'organisateur du scrutin, l'OAE, mais aussi éventuellement par diverses institutions accréditées (Conseil de l'Europe, partis politiques, conseils locaux, etc.). Ce principe présente l'avantage de protéger le scrutin contre les menaces internes ; ainsi, même un gouvernement

[3] Source : Wikipédia, https://fr.wikipedia.org/wiki/Blockchain.

[4] Par exemple, la ville de Zoug en Suisse a effectué un vote fictif par chaînes de blocs du 25 juin au 1er juillet 2018. Voir le rapport d'évaluation ici : http://www.stadtzug.ch/dl.php/de/5c00ff8dbd830/eVoting_Final_Report_ENG.pdf

corrompu ne pourrait pas, semble-t-il, falsifier les votes. Une fois enregistré, un vote ne peut être ni supprimé ni modifié, car la chaîne de blocs est, de l'avis de ses concepteurs, immuable. Lorsque le nombre de nœuds (dans la grappe) est suffisamment grand, le système est, semble-t-il, protégé contre le piratage. Les identités des électeurs étant anonymisées, le vote est censé être secret. Cela dit, ce point est sujet à caution, car l'identité d'une personne peut être pistée au moyen des informations relatives à son adresse publique et grâce à son IP. Cette technologie soulève en outre d'autres questions comme l'interopérabilité, les coûts, etc.

La chaîne de blocs est de plus en plus utilisée pour mettre en œuvre des processus dans lesquels les enregistrements ou les transactions, les contrats et les documents officiels doivent être inaltérables, persistants et interrogeables. Ainsi, certaines administrations l'utilisent pour les cadastres, les transactions officielles, etc. (en Suède et dans le canton de Genève par exemple). On peut imaginer que les administrations qui ont recours à ce mécanisme pourraient être tentées de l'utiliser aussi pour le cycle électoral, par exemple pour tenir à jour les listes électorales, le registre des partis politiques, etc. Du reste, lorsque les registres d'état civil sont basés sur une chaîne de blocs, il y a toutes les chances que la liste électorale qui en est extraite le soit aussi. Ainsi la mise en place d'une chaîne de bloc pour gérer une composante du cycle électoral aura-t-elle une incidence sur l'ensemble du cycle.

Informatique en nuage

L'informatique en nuage désigne la possibilité de disposer, à la demande, de ressources systèmes informatiques (stockages de données et puissance de calcul en particulier), sans que l'utilisateur ait à les gérer directement et de manière active. En règle générale, cette expression est utilisée pour désigner des centres de traitement de données mis à la disposition de nombreux utilisateurs via internet[5]. Les nuages peuvent être privés ou publics.

Des organisations (notamment des entreprises) ont déjà transféré leur informatique vers le nuage, ou envisagent de le faire, car cette solution est supposée plus économe et plus sûre que la conservation des capacités informatiques dans l'organisation. Dans le cas des systèmes critiques comme la gestion des élections, le transfert vers le nuage pose problème, car les autorités doivent garder le contrôle et, de préférence, posséder une expertise informatique et mettre en œuvre des solutions en interne ; telle est du moins l'opinion courante aujourd'hui. Les questions qui se posent concernent la protection des données, la sécurité des documents et des processus sensibles et l'obligation de rendre des comptes. L'informatique en nuage est un facteur de nouvelles vulnérabilités (sur le plan de la sécurité, de la confidentialité et du respect de la vie privée notamment) et expose à un risque d'attaques. Le travail des experts en criminalistique et les enquêtes sur les irrégularités sont donc plus complexes. Il est à noter qu'à ce jour, le recours à l'informatique en nuage pour la gestion des documents et des processus du cycle électoral n'a pas fait l'objet d'études spécifiques.

[5] Wikipédia, https://fr.wikipedia.org/wiki/Cloud_computing.

Intelligence artificielle

L'intelligence artificielle (IA) fait référence à un ensemble de méthodes, dont certaines existent déjà, tandis que d'autres sont à l'état d'hypothèses[6]. L'IA se rapporte à des systèmes qui manifestent un comportement intelligent en analysant leur environnement et en agissant — avec un certain degré d'autonomie — pour atteindre des buts précis[7]. Le domaine de l'IA reprend des éléments de nombreux autres domaines. Les thèmes habituels de la recherche sur l'IA comprennent le raisonnement et la prise de décision (représentation des connaissances, planification, ordonnancement, recherche, optimisation), l'apprentissage (apprentissage automatique, réseaux neuronaux, apprentissage profond, arbres de décision, etc.) et la robotique (IA embarquée, capacité à se déplacer et à interagir avec le monde physique). Pour l'heure, les solutions mettant en œuvre l'IA sont propres à un domaine ; l'intelligence générale fait partie des objectifs à long terme.

À notre connaissance, aujourd'hui, l'IA n'est pas utilisée dans le cycle électoral. L'utilisation d'une intelligence artificielle générale dans le futur (en supposant qu'elle existe un jour) en vue d'améliorer la prise de décision sonnerait quasiment la fin de la démocratie telle que nous la connaissons aujourd'hui. Cela étant, les techniques d'IA sont de plus en plus utilisées dans d'autres domaines, notamment la justice. Ainsi, les systèmes appelés « tribunaux virtuels » ou « justice prédictive » sont actuellement utilisés pour conseiller les juges (au Canada par exemple).

Les grandes problématiques qui touchent à l'IA concernent notamment les données et l'explicabilité. S'agissant des données, les systèmes d'IA ont besoin, pour être efficaces, de traiter de grands volumes de données et leur fiabilité dépend de la qualité des données avec lesquelles on les alimente. Une intelligence artificielle qui baserait son apprentissage sur des données d'entraînement biaisées (pas assez inclusives par exemple) serait inéquitable et produirait des décisions injustes. L'explicabilité, quant à elle, fait référence à la nature opaque de certains systèmes d'IA, c'est-à-dire à l'impossibilité pour les ingénieurs de comprendre comment ces systèmes parviennent à telle ou telle décision. Il est de plus en plus admis, à l'échelon des pays et au niveau international, que les systèmes d'IA doivent absolument être conçus de telle manière que leurs décisions puissent être expliquées et que la responsabilité incombe toujours à l'être humain[8].

L'intelligence artificielle pourrait avoir une incidence sur les solutions de nouvelles technologies utilisées pour les élections. Par exemple, elle pourrait servir à mener des cyberattaques encore plus perfectionnées et difficiles à prévoir, « susceptibles notamment de poursuivre des objectifs hautement personnalisés et capables de s'adapter en temps réel[9]. » Les OAE devraient prendre ce risque très au sérieux. Dans le même temps, il est probable que l'IA sera entraînée et utilisée à des fins de cyberdéfense.

---

[6] Service de recherche du Parlement européen (2019), *How artificial intelligence works*. Voir aussi Wikipédia, https://fr.wikipedia.org/wiki/Intelligence_artificielle.

[7] Commission européenne, Groupe d'experts de haut niveau indépendants sur l'intelligence artificielle, *A definition of AI: Main capabilities and disciplines*, 8 avril 2019.

[8] Recommandation 3C du rapport du groupe de travail de haut niveau des Nations Unies, *The age of digital interdependence*, juin 2019 ; États-Unis, loi de 2019 intitulée *Algorithmic accountability act* (loi relative à la responsabilité algorithmique) ; Gouvernement allemand, *Strategie Künstliche Intelligenz der Bundesregierung*, novembre 2018 ; Cédric Villani (France), rapport *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, mars 2018.

[9] Rapport du groupe de travail de haut niveau des Nations Unies, *The age of digital interdependence*, juin 2019.

Sous l'angle du cycle électoral

Législation

Cette partie du cycle électoral comprend la conception et la rédaction de toutes les lois et règles relatives aux élections à tous les niveaux de gouvernance et de tous types : droit formel et droit matériel, voire codes de conduite et autres instruments pouvant avoir une incidence directe ou indirecte sur les élections. Ces éléments n'étant pas tous proposés ou rédigés par l'OAE, il est important que cette dernière ait une vue d'ensemble structurée et claire de tous les éléments réglementaires à prendre en compte dans le processus électoral.

Le rôle des nouvelles technologies dans ce domaine est, pour l'essentiel, de préparer, d'organiser et d'extraire des informations. Mais surtout, la législation devrait réglementer l'utilisation de ces technologies dans le cycle électoral. Ainsi que l'ont montré les arrêts des cours constitutionnelles relatifs au vote électronique en Allemagne et en Autriche, il s'est révélé difficile d'élaborer des règles qui respectent des principes de niveau supérieur, et ce d'autant plus qu'il demeure des incertitudes quant à la façon dont les principes s'appliquent aux nouvelles technologies. Que faut-il inclure dans la réglementation pour qu'elle soit en conformité ? Comment gérer la légalité ou la sécurité juridique, au vu de la complexité des nouvelles technologies et de leur évolution rapide, qui est dictée par les besoins de l'industrie ? Comment contrôler la conformité ? Etc.

L'une des difficultés concerne les concepts utilisés. Dans un monde analogique, la sécurité et les contrôles, par exemple, sont envisagés de façon statique (comme les produits), alors que dans un contexte de haute technologie, ils doivent s'adapter au jour le jour pour répondre à l'évolution des vulnérabilités et des menaces et donc aux nouveaux risques qui se présentent. Certains comparent cette situation à une course aux armements. La réglementation rend compte ou devrait rendre compte de cette particularité. Dans le monde analogique, les OAE doivent garantir la sécurité, sauf dans des cas exceptionnels comme la force majeure. Mais comment définir leur rôle dans un contexte numérique ? Il est facile d'accepter la force majeure dans les contextes de faible technicité. Les aléas sont-ils acceptables dans le logiciel (s'agissant de l'IA) ? Quelles garanties un OAE devrait-il apporter, sachant que les nouvelles technologies évoluent par tâtonnements ? Quelles obligations positives découlent du fait qu'il doit assurer la conformité avec l'article 3 du Protocole n° 1 de la CEDH dans le cycle électoral ?

Les réponses ne sont pas triviales, tant s'en faut. Les cours constitutionnelles (Allemagne, Autriche, etc.), les parlements, les gouvernements et les organisations de contrôle (Pays-Bas, Norvège, France, etc.) reconnaissent les lacunes de la réglementation en vigueur, par exemple en matière de vote électronique. Ces réglementations, héritées des années 1970, 1980 et 1990, doivent évoluer pour prendre en compte les technologies les plus récentes. Dans quelques pays seulement (Belgique, Estonie, Suisse, etc.), l'autorité de réglementation a actualisé les textes réglementaires. Mis à l'épreuve de la pratique pour contrôler leur adéquation, il apparaît qu'ils doivent encore évoluer (voir par exemple l'exercice de transparence mené en Suisse en 2019 ainsi que les enseignements tirés en matière de vérifiabilité, de transparence et de certification). Les recommandations formulées par le Conseil de l'Europe ont joué un rôle capital en incitant les États à actualiser leur réglementation. Cela étant, la dernière vague de questions n'a pas encore été examinée au sein du CAHVE de l'Organisation (Comité ad hoc d'experts sur les normes juridiques, opérationnelles et techniques relatives au vote électronique) : Comment vérifier et contrôler les mécanismes de vérification ? Comment évaluer les postulats relatifs à la confiance, qui sont nécessaires dans le vote électronique vérifiable ? Comment paramétrer la transparence (que se passe-t-il après la publication du code source) ? Etc. Un forum de discussions et d'échanges continus s'impose, car c'est par la pratique que nous apprenons.

Le vote électronique est le domaine de réglementation des nouvelles technologies le plus évolué. À l'heure actuelle, La plupart des autres solutions de haute technologie utilisées dans le cycle électoral sont encore réglementées, au mieux, selon une approche étroite de la gestion informatique, et certaines ne sont pas réglementées du tout. Leur conformité avec l'article 3 du Protocole n° 1 à la CEDH et avec les principes électoraux nationaux n'a, à ce jour, pas été remise en question. Les efforts déployés par les OAE pour actualiser la réglementation se sont heurtés à une vive résistance (voir à ce sujet les échanges de vues sur la réglementation des solutions de dépouillement électronique en Suisse et la résistance des cantons). Cela étant, les choses évoluent rapidement depuis qu'en 2016, des pays étrangers sont parvenus à s'immiscer dans des élections en « piratant » des solutions électroniques utilisées dans le cycle électoral, ce qui avait fait grand bruit. Des événements récents survenus lors des élections de 2017 aux Pays-Bas (dépouillement des bulletins de vote et décompte des voix) et en Allemagne (logiciel de transmission des résultats) montrent que des processus de la plus haute importance pour le résultat des élections souffrent de problèmes analogues à ceux qui touchent le vote électronique et qu'ils devraient être mieux réglementés. Un consensus se dégage aujourd'hui en faveur d'une meilleure réglementation. C'est l'occasion où jamais pour le Conseil de l'Europe de continuer d'apporter son aide et ses conseils, en s'appuyant sur les travaux menés dans le domaine du vote électronique, qui, semble-t-il, est l'utilisation la plus complexe des nouvelles technologies dans le contexte électoral.

Planification et financement

L'OAE supervise les différentes étapes du cycle électoral : calendrier des élections, recrutement et formation du personnel, logistique et sécurité, politiques électorales nationales ou régionales, services électoraux, passation des marchés pour les services externalisés, recrutement et formation du personnel électoral, etc. À cette fin, il bénéficie d'un soutien informatique adapté à ses besoins. Les principales questions qui se posent ici sont les suivantes : Dans quelle mesure les solutions mises en place sont-elles à l'épreuve des pirates informatiques (sécurité) ? Dans quelle mesure les processus du cycle électoral dépendent-ils de ces solutions ? Quelles sont les solutions de repli proposées.

Éducation, information, réglementation de la conduite à tenir

En règle générale, c'est l'OAE qui est chargé d'informer et d'éduquer les électeurs et les citoyens. Il œuvre en faveur de l'accès à tous, encourage la mise en place de politiques et de pratiques d'égalité et d'équité, et peut aussi fournir des moyens de recherche en matière électorale. En plus de ses activités en direction des électeurs, il recrute et forme le personnel électoral temporaire. L'OAE accrédite les observateurs et définit leurs modalités de travail. Il forme les scrutateurs des partis politiques et des candidats, fournit un accès aux médias et réglemente la conduite des médias pendant les élections et les enquêtes d'opinion.

L'informatique vient en support de ces activités. Les questions recensées sous le chapitre « planification et financement » s'appliquent aussi ici.

Inscription

On distingue deux grands types de registres : les listes électorales (listes des électeurs) et les registres des partis politiques. Pendant le vote, l'exercice des droits de vote (le fait qu'une personne a voté) est également enregistré. Lorsque la liste électorale est élaborée sur la base d'une inscription, l'autorité compétente doit déterminer si l'électeur a effectivement le droit de voter. Les listes électorales comprennent les électeurs résidant dans le pays, les électeurs qui résident à l'étranger et ont le droit de voter, et, parfois, des étrangers établis dans le pays. L'OAE enregistre aussi les forces politiques (partis, mouvements, etc.). Avant chaque élection, il reçoit et valide les candidatures. Il peut aussi superviser les présélections ou primaires des partis politiques.

La question de l'identification unique des personnes (électeurs et candidats) se pose pour tous les registres. L'identification unique permet de garantir le suffrage égal (un vote par personne) et le respect des règles électorales relatives à la candidature. Dans les systèmes analogiques, les personnes sont identifiées manuellement : cette procédure est lourde et sujette aux erreurs de vérification. Dans le monde numérique, les solutions électroniques permettent, entre autres avantages, d'effectuer une vérification rapide et de prévenir efficacement les votes ou les candidatures multiples. Outre la biométrie (voir plus haut), une autre solution (peu courante) appelée « identification électronique unique » fait l'objet de débats. Certains pays ont aussi tenté d'utiliser d'autres identifiants uniques, habituellement le numéro de sécurité sociale. Jusqu'ici, la mise en place d'identifiants électroniques dans le cycle électoral et l'utilisation d'autres identifiants uniques comme le numéro de sécurité sociale se sont vues opposer une vive résistance, essentiellement de la part des organismes de surveillance garants de la protection des données, qui a toujours primé sur le respect d'autres principes et règles définis sur la base de l'article 3 du Protocole n° 1. Mais on a observé récemment que ces organismes étaient plus ouverts à l'utilisation de tels principes et règles et que les identifiants électroniques étaient plus souvent utilisés, car ils sont censés faciliter les transactions dans tous les domaines de la vie. Cette évolution témoigne de l'importance accrue de la protection des données utilisées pendant les élections.

Vote, dépouillement, vérification et publication des résultats

Cette étape correspond au processus électoral en tant que tel, qui couvre l'ouverture et la clôture du scrutin ainsi que le dépouillement, la vérification et la publication des résultats. Ce processus comprend plusieurs étapes, notamment, le cas échéant, l'identification électronique des électeurs, le vote électronique, le dépouillement électronique et la transmission électronique des résultats. Le Conseil de l'Europe a fait œuvre de pionnier en matière de vote et de dépouillement électroniques (voir la Recommandation Rec(2017)5 et les lignes directrices associées).

Même dans les pays qui n'ont pas mis en place le vote électronique, les OAE utilisent des logiciels pour planifier et accomplir certaines tâches, par exemple des audits et des activités destinées à contrôler l'exactitude des résultats. À cet égard, il existe des méthodes statistiques permettant de vérifier que les résultats sont plausibles (la Commission de Venise a également étudié cet aspect). Dans le cas de l'intelligence artificielle, les méthodes statistiques doivent être « alimentées » avec des données numérisées concernant les élections en cours et les élections passées. À partir de ces données, elles tirent des conclusions sur l'exactitude des résultats. Là encore, la qualité et la quantité des données sont essentielles au fonctionnement optimal de ces méthodes.

Résolution des contentieux

Il arrive que l'OAE soit l'autorité compétente en matière de résolution des contentieux. Dans ce cas, il peut recourir à des solutions basées sur les nouvelles technologies pour obtenir les informations dont il a besoin. On ne parle pas encore de justice prédictive, mais certains outils d'extraction d'informations présentent un intérêt dans la mesure où ils peuvent aider les OAE à prendre des décisions rapides et correctes. Sans doute ces outils permettront aux électeurs de mieux comprendre leurs droits. Ils peuvent aussi améliorer l'accès des requérants à la justice (électeurs, partis, etc.).

Fonctions postélectorales

Il s'agit notamment d'actualiser les données et les outils, de passer en revue le cadre électoral et d'en évaluer l'adéquation, d'estimer la qualité du travail de l'OAE et de conseiller le gouvernement et l'organe législatif sur des questions de réforme électorale. Les observations formulées plus haut à propos de la planification s'appliquent aussi aux fonctions postélectorales.

Questions transversales

Certaines questions transversales comme la protection des données ou la sécurité des systèmes informatiques et des informations sont couvertes par des instruments existants. Cela étant, les élections restent un cas à part, auquel s'appliquent des exigences spécifiques (plus strictes), qui devraient être formulées dans une réglementation spéciale.

Protection des données

L'instrument général applicable dans la région est la Convention 108+ pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, qui tient compte de plusieurs autres instruments internationaux en vigueur. Au niveau de l'UE, le principal instrument est le règlement général (UE) 2016/679 sur la protection des données (RGPD). Les dispositions de ces textes traitent de l'utilisation illégale de données à caractère personnel également dans le contexte électoral. La Convention 108+ du Conseil de l'Europe et le RGPD de l'UE ont été élaborés en parallèle et sont mutuellement compatibles. Le RGPD complète certains principes de la Convention 108+.

Cela dit, les données utilisées pendant les élections ou liées aux opinions politiques sont une catégorie de données sensibles bien particulière. Leur traitement ne doit être autorisé que si des garanties appropriées sont prévues par des lois (article 6 de la Convention 108+). Pour rédiger ces lois, les OAE et le législateur en général doivent avoir des connaissances spécialisées qui se conjuguent. Par exemple, l'utilisation de la cryptographie est une mesure importante pour protéger certaines de ces données. Des lignes directrices pourraient être utiles dans ce domaine.

(Cyber)sécurité.

La cybersécurité est un sujet relativement récent pour les OAE. Des réglementations portant sur la cybersécurité des infrastructures essentielles sont actuellement mises en place au niveau des pays. On observe en outre une tendance à déclarer les infrastructures essentielles utilisées pour les élections (voir les États-Unis ou la Suède ; les initiatives de l'UE concernant les élections du parlement de l'Union en 2019 vont dans le même sens). Les OAE doivent veiller à ce que les règles et principes électoraux soient respectés lorsque des mesures de cybersécurité sont mises en place et appliquées.

Coopération public-privé

La coopération public-privé est un aspect important de l'utilisation des nouvelles technologies dans le cadre des élections. En fait, la plupart des solutions mettant en œuvre ces technologies sont élaborées par des entreprises privées, qui se chargent aussi de les contrôler. Au moment de mettre en place le vote électronique par exemple, l'OAE devrait veiller à ce que les conditions relatives à la passation des marchés comprennent des exigences essentielles à la conformité des systèmes et des solutions avec l'article 3 du Protocole n° 1 de la CEDH.

Un aspect important concerne la clarification des responsabilités. La responsabilité politique devrait incomber à l'OAE. Cela étant, en cas d'erreur avérée, il convient de déterminer à qui incombe la responsabilité et ce point doit être précisé avant le début de la coopération. On citera ici, comme exemple récent, l'exercice de transparence effectué en Suisse au début de l'année : les garanties offertes par le fournisseur et par l'autorité de certification s'étant révélées partiellement erronées, le vote électronique n'a pas été utilisé lors du scrutin de mai ni lors de l'élection d'octobre. Certains cantons ont déclaré qu'ils avaient l'intention de poursuivre le fournisseur en justice[10].

[10] Driza Maurer Ardita (2019), « The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation », dans R. Krimmer et autres (dir.), E-Vote-ID 2019, LNCS 11759, p. 83 à 99, 2019.

RECOMMANDATIONS

Compte tenu de l'utilisation actuelle des nouvelles technologies dans le cadre électoral et de l'usage qui pourrait en être fait à l'avenir, les quatre scénarios suivants proposent des recommandations que le Conseil de l'Europe pourrait éventuellement adresser dans le futur.

Scénario 1 : Cadre d'échanges multidisciplinaires

Accroître la dépendance aux nouvelles technologies

L'existence des technologies numériques et leur application à tous les aspects de la vie, ou presque, y compris aux élections, sont aujourd'hui un fait qui ne peut être nié (Commission de Venise, 2019).

De plus, on observe actuellement une tendance à adopter des technologies toujours plus récentes pour résoudre de vieux problèmes (exemple : mise en place de chaînes de blocs pour garantir que les votes ou les documents tels que les registres ne peuvent pas être modifiés) ou pour résoudre des problèmes qui sont apparus avec l'utilisation des nouvelles technologies (algorithmes d'IA entraînés pour se protéger des cybermenaces, etc.).

En ce qui concerne l'utilisation des nouvelles technologies dans le cycle électoral, on observe à l'heure actuelle, dans les États membres et dans l'ensemble de la région, une grande multiplicité de documents, de solutions et d'approches. Si ce développement « organique » apporte un éclairage précieux sur la situation, il est nécessaire, face au risque de perte de contrôle, de passer en revue et de consolider les réglementations, de renforcer leur conformité avec l'article 3 du Protocole n° 1 à la CEDH et d'adapter le cycle électoral pour qu'il résiste aux risques liés aux nouvelles technologies (et, on peut l'espérer, qu'il en exploite toutes les possibilités).

Les nouvelles technologies sont aujourd'hui sur toutes les lèvres et les OAE ont besoin d'un cadre de discussion multidisciplinaire et structuré pour examiner les questions qu'elles posent.

La discussion a lieu au niveau national, là où s'exercent les responsabilités liées à l'organisation des élections. Pourtant, en règle générale, les OAE ne disposent ni de l'expertise multidisciplinaire, ni des ressources humaines, des moyens financiers et du temps nécessaires pour traiter eux-mêmes la question de façon approfondie. Et quand bien même ils le pourraient, il serait hautement souhaitable de coordonner les solutions à grande échelle.

Les lignes directrices du Conseil de l'Europe sur le vote électronique — qui est l'aspect le plus complexe du cycle électoral — pourraient être étendues pour traiter aussi de l'utilisation des nouvelles technologies sur l'ensemble du cycle. Compte tenu de sa mission, le Conseil de l'Europe est l'organisation la plus à même d'aider techniquement et concrètement les États membres à édicter une réglementation garantissant que l'utilisation des nouvelles technologies est bien conforme à l'article 3 du Protocole n° 1 à la CEDH.

Un processus axé sur les droits de l'homme

« Les valeurs communes sont encore plus importantes pendant les périodes de grands changements et d'imprévisibilité et lorsque les informations sont limitées [...] Il serait utile que le secteur privé, les collectivités et les gouvernements mènent des initiatives de coopération numérique en définissant expressément les valeurs et les principes qui les guident[11]. »

[11] Rapport du groupe de haut niveau des Nations Unies (2019, p. 30).

Le Conseil de l'Europe a pour mission de veiller au respect de la CEDH, ce qui couvre aussi les élections et le respect de l'article 3 du Protocole n° 1. Dans le monde actuel, cet aspect se traduit par la publication d'orientations sur la façon de mettre en œuvre et de respecter les principes d'élection libre lorsque les nouvelles technologies sont utilisées. L'Organisation a déjà une grande expérience en matière de respect des élections libres dans le contexte du vote électronique (voir les Recommandations de 2004 et 2017 sur le vote électronique). Le vote (électronique) étant le processus le plus complexe du cycle électoral, l'Organisation a déjà beaucoup travaillé sur la définition de la signification des principes dans un contexte de vote électronique et sur l'opérationnalisation des principes par l'élaboration de lignes directrices détaillées. Cette expertise pourrait s'étendre à l'ensemble du cycle. Il conviendrait de veiller à l'application des droits de l'homme dès la conception. Aussi les discussions sur la conformité devraient-elles s'engager dès le début de l'élaboration des solutions fondées sur les nouvelles technologies.

En envisageant ainsi son action d'aide et de conseil, l'Organisation contribue à renforcer les capacités humaines et institutionnelles au niveau des OAE pour que l'utilisation des nouvelles technologies soit conforme aux principes, en synergie avec d'autres travaux qu'elle mène sur les élections (ElecData par exemple), dans le but d'améliorer la transparence des réglementations, l'évaluation croisée et l'harmonisation. Elle offre aux États et aux autres acteurs concernés un « service d'assistance et d'information » qui leur permet de comprendre les problématiques numériques dans le contexte électoral et de respecter les principes afin de maximiser les avantages et de réduire les préjudices au minimum. Elle contribue à garantir que les solutions numériques ont pour socle le respect du droit à des élections libres et le respect des autres droits de l'homme.

Holistique et multidisciplinaire

En tant que coordonnateur, le Conseil de l'Europe offre une enceinte sans équivalent non seulement pour débattre des principes, mais aussi pour mener des réflexions multidisciplinaires, et ce au niveau régional. En matière de vote électronique comme dans de nombreux autres domaines, un consensus de plus en plus large se dégage sur la nécessité d'adopter une approche « système ». Comme les solutions, les risques et les opportunités sont interdépendants. La coopération et la réglementation doivent être multi-parties prenantes et évolutives. Il est donc nécessaire de mettre en place une plate-forme ou un forum pour débattre de ces questions, compte tenu en particulier de la complexité des nouvelles solutions telles que l'intelligence artificielle. La création d'un forum spécialisé répond au souhait et à la nécessité d'obtenir des résultats plus concrets, de faire participer plus activement les pouvoirs publics et le secteur privé, de mettre en place des processus plus inclusifs et d'assurer un suivi plus efficace.

Scénario 2 : Orientations générales concernant certains aspects de la protection des données

Dans ce domaine, les travaux porteraient essentiellement sur la protection des données qui alimentent les solutions à base de nouvelles technologies. Ici, la question est de savoir ce qu'entraîne le respect des principes (droit à des élections libres), en particulier le respect du suffrage égal. On l'a vu plus haut, les données utilisées lors des élections sont des données qualifiées. Des exigences spéciales s'appliquent, qui doivent être plus contraignantes que celles posées par la Convention 108+ et le RGPD. Mais très souvent, les responsables ne savent pas avec certitude quelles sont ces exigences, preuve que ces préoccupations sont relativement nouvelles pour les OAE. Elles sont aussi complexes, compte tenu de l'interaction entre les différents instruments existants et les spécificités des élections. En précisant comment les grandes catégories de données utilisées lors des élections doivent être gérées, le nouveau document d'orientation comblerait cette lacune.

L'adoption d'une démarche transversale oblige les OAE à suivre une approche holistique et à examiner l'ensemble des données qui sont en leur possession. La protection des données devrait en être améliorée.

Scénario 3 : Orientations générales concernant certains aspects de la sécurité

Les principes concernant la protection des données s'appliquent aussi à la sécurité des solutions à base de nouvelles technologies. Là encore, la question est transversale. Les OAE doivent réfléchir à la sécurité des solutions, à la sécurité du matériel et aux effets que pourraient avoir la corruption, l'interruption, etc., du matériel sur les élections en cours. À cet égard, des procédures de sauvegarde sont prévues.

Certaines villes et administrations ont déjà été victimes d'un blocage de leurs processus administratifs par des logiciels rançonneurs (voir par exemple Baltimore en mai 2018). Ces exemples montrent ce qui peut dysfonctionner en cas d'attaque, et comment des processus essentiels peuvent devenir la cible de pirates dont la motivation est politique, financière ou autre.

Par ses recommandations, le Conseil de l'Europe pourrait aider les États à mettre leur législation générale relative à la cybersécurité et aux infrastructures essentielles en adéquation avec les spécificités du domaine électoral.

Les scénarios 1, 2 et 3 sont complémentaires. Pour rester pleinement pertinentes, les lignes directrices sur la protection des données ou la sécurité lors des élections doivent être réexaminées en permanence, d'où la nécessité d'un forum de discussion.

Scénario 4 : Pas de nouvelles recommandations

Dans ce scénario, nous nous plaçons dans l'hypothèse où aucune nouvelle recommandation n'est édictée. On peut supposer que le Conseil de l'Europe continuera de travailler sur le vote électronique, comme le prévoit la Recommandation Rec(2017)5. La plupart des questions peuvent être examinées dans ce cadre, à condition qu'un forum de discussion (réunions périodiques) soit mis en place. Toutefois, les échanges resteront focalisés sur le vote électronique et les spécificités des autres éléments du cycle seront laissées de côté.

D'autres parties prenantes, essentiellement des fournisseurs et d'autres organisations internationales, continueront de travailler sur le sujet et occuperont le terrain[12]. Mais malgré tout le mérite qu'on peut leur reconnaître, ces organisations n'ont pas le mandat du Conseil de l'Europe ni la possibilité de produire des lignes directrices sur la manière de réglementer l'utilisation des nouvelles technologies dans les élections.

D'autres organes du Conseil de l'Europe continueront de travailler sur différentes questions liées aux élections. Le Comité de la Convention de Budapest en est un bon exemple. Mais ces initiatives resteront éparses (et non systémiques et holistiques), car la Convention de Budapest, par exemple, ne traite que d'un aspect particulier (mais important) de la cybersécurité, en l'occurrence la coopération interétatique en réponse aux violations.

[12] Très récemment, l'UNESCO/PNUD a commencé à travailler sur une publication intitulée *Elections and Internet, Social Messaging and AI – Guide for Electoral Practitioners*. Citons également la Commission mondiale des Nations Unies sur la stabilité dans le cyberespace, qui est en train d'élaborer des propositions, entre autres, pour la non-ingérence dans les élections et la mise en place d'un accord par lequel les signataires s'engageraient à ne pas attaquer les infrastructures essentielles (Rapport du groupe de haut niveau des Nations Unies, 2019, p. 27).

Choix de références

Conseil de l'Europe, Comité d'experts (MSI-AUT), *Projet de Recommandation du Comité des Ministres aux États membres sur les conséquences des systèmes algorithmiques pour les droits de l'homme*, 26 juin 2019.
Conseil de l'Europe, *Convention 108+*, *Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, juin 2018.
Conseil de l'Europe, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Rapport sur l'intelligence artificielle. Intelligence artificielle et protection des données : enjeux et solutions possibles*, 25 janvier 2019.
Conseil de l'Europe, Comité de la Convention sur la cybercriminalité (T-CY), *Note d'orientation #9. Aspects de l'ingérence électorale au moyen de systèmes informatiques couverts par la Convention de Budapest*, 8 juillet 2019.
Conseil de l'Europe, *Déclaration du Comité des Ministres sur les capacités de manipulation des processus algorithmiques*, 13 février 2019.
Conseil de l'Europe, *Recommandation Rec(2017)5 du Comité des Ministres aux États membres sur les normes relatives au vote électronique*.
Commission européenne, *Des élections libres et régulières. Document d'orientation. Orientations de la Commission relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral*. La contribution de la Commission européenne à la réunion des chefs d'État et de gouvernement à Salzbourg les 19 et 20 septembre 2018.
Commission européenne, Groupe d'experts de haut niveau sur l'intelligence artificielle, *A definition of AI : Main capabilities and disciplines*, 8 avril 2019.
Commission européenne pour la démocratie par le droit (Commission de Venise) et autres, *Draft Joint Report on Digital Technologies and Elections*, 7 juin 2019.
IDEA, *Cybersecurity in elections. Models of interagency cooperation*, 2019.
IDEA, *Electoral Management Design,* édition révisée, 2014
OSCE/BIDDH, *Handbook for the observation of new voting technologies,* 2013.
Groupe de travail de haut niveau du Secrétaire général des Nations Unies, *The age of digital interdependence*, juin 2019.