COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DÉLÉGUÉS DES MINISTRES Documents CM CM(2017)50-add1final 14 juin 2017

1289e réunion, 14 juin 2017

Démocratie et questions politiques

2.3 Comité ad hoc d'experts sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (CAHVE)

a. Exposé des motifs de la Recommandation CM/Rec(2017)5 du Comité des Ministres aux États membres sur les normes relatives au vote électronique

Point examiné par le GR-DEM lors de ses réunions du 20 avril et 1er juin 2017

Contexte

1. La présente recommandation sur les normes relatives au vote électronique et son exposé des motifs sont la version mise à jour de la « Recommandation Rec(2004)11 du Comité des Ministres aux États membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique » et de son exposé des motifs, qui avaient été adoptés le 30 septembre 2004. En 2010, deux documents complémentaires ont été approuvés : les Lignes directrices pour la conception de processus de confirmation du respect des exigences et normes recommandées (certification des systèmes de vote électronique) et les Lignes directrices relatives à la transparence des élections par voie électronique.

2. La Recommandation Rec(2004)11 et les lignes directrices qui l'accompagnent ont servi de points de repère juridiques aux pays et institutions de la région pour instaurer, gérer et évaluer les systèmes de vote électronique. À la suite des conclusions des réunions biennales de 2012 et 2014 consacrées à l'examen de la Rec(2004)11 et d'une réunion d'experts organisée à Vienne en décembre 2013, le Comité des Ministres a décidé le 1er avril 2015, en vertu de l'article 17 du Statut du Conseil de l'Europe et conformément à la Résolution CM/Res(2011)24 concernant les comités intergouvernementaux et les organes subordonnés, de créer un « Comité ad hoc d'experts sur les normes juridiques, opérationnelles et techniques relatives au vote électronique » (CAHVE).

3. Le CAHVE avait pour mandat de préparer une nouvelle recommandation mettant à jour la Recommandation Rec(2004)11 et son exposé des motifs à la lumière des récentes évolutions techniques et juridiques en matière d'élections par voie électronique au sein des États membres du Conseil de l'Europe. La mise à jour devrait viser à améliorer et développer la Recommandation Rec(2004)11, en remédiant aux lacunes constatées dans la recommandation, en s'appuyant sur les récentes expériences de vote électronique dans la région et en tenant compte des implications des concepts et solutions techniques émergents. Le processus de mise à jour devrait être axé sur une évaluation des besoins, en se basant notamment sur les points de vue des États membres et des parties prenantes non gouvernementales. Conformément à son mandat, le CAHVE a élaboré les documents suivants : la Recommandation Rec(2017)XX du Comité des Ministres aux États membres sur les normes relatives au vote électronique, qui révise et remplace la Recommandation Rec(2004)11 sur les normes juridiques, opérationnelles et techniques, et le présent exposé des motifs. En plus de son mandat, le CAHVE a préparé des « Lignes directrices pour la mise en œuvre des dispositions de la Recommandation Rec(2017)XX sur les normes relatives au vote électronique ».

4. La présente recommandation contient des normes sur le vote électronique qui reflètent les principes des élections et référendums démocratiques et les transposent au vote électronique. Ces règles visent à garantir le respect de ces principes dans le cadre du vote électronique et à donner ainsi confiance dans les systèmes nationaux de vote électronique.

5. Les principes régissant les élections et référendums démocratiques découlent des instruments du Conseil de l'Europe et d'autres instruments internationaux en vigueur dans le domaine électoral. Les normes fixent des objectifs que le vote électronique doit permettre d'atteindre pour respecter les principes susmentionnés. Elles sont communes à toute la région du Conseil de l'Europe.

6. La souveraineté des États membres du Conseil de l'Europe en matière d'élections et de référendums n'est pas touchée par la présente recommandation, qui porte sur le recours au vote électronique lors des élections et des référendums politiques. Ces derniers peuvent avoir lieu à différents niveaux et certains pays n'organisent aucun référendum. Les normes s'appliquent de la même manière, que le vote électronique soit utilisé pour une élection politique ou pour un référendum politique.

7. Les raisons d'introduire ou d'envisager d'introduire le vote électronique varient d'un pays à l'autre et dépendent du contexte national propre à chaque pays. Il est clair aujourd'hui que l'instauration d'un système de vote électronique ne peut se faire qu'à la condition que les électeurs aient pleinement confiance dans leur système électoral et leur administration électorale. La présente recommandation n'impose pas aux États membres d'introduire un dispositif de vote électronique. Elle fait le constat qu'un nombre croissant de pays recourent en partie au vote électronique ou envisagent de le faire dans un proche avenir. Elle énonce des normes qui visent à harmoniser la mise en œuvre des principes relatifs aux élections et référendums démocratiques lorsque le vote électronique est en usage dans les États membres.

8. Dans la présente recommandation, le terme « vote électronique » renvoie à l'utilisation de moyens électroniques aux fins du vote et du décompte, dans des environnements contrôlés ou non. Il englobe les machines de vote électronique dans les bureaux de vote, l'utilisation de scanners optiques pour enregistrer et/ou compter les bulletins de vote, ainsi que le vote électronique à distance. Sauf mention particulière, les normes s'appliquent à toutes les formes de vote électronique. Celles qui concernent une seule ou plusieurs formes le précisent. Des dispositions de mise en œuvre détaillées, souvent propres à une forme de vote électronique, figurent dans les « Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique ».

9. Les systèmes électoraux peuvent conjuguer vote local et vote à distance. Le vote à distance peut s'effectuer dans un environnement contrôlé (ambassade, consulat, bureau de poste, mairie, etc.) ou non contrôlé, c'est-à-dire non surveillé par des représentants des services électoraux (par exemple, le vote depuis chez soi par correspondance ou depuis un ordinateur sur internet). Chaque État membre a sa propre pratique établie concernant les modes de suffrage proposés aux électeurs[1]. Aux fins de la présente recommandation, le « vote électronique à distance » désigne l'utilisation de moyens électroniques pour exercer son suffrage en dehors des locaux où le vote se déroule habituellement.

10. La recommandation aborde divers aspects du vote électronique aux différentes phases du processus électoral ou référendaire (avant, pendant et après le scrutin), ainsi que les rôles et responsabilités des parties prenantes. Les normes qu'elle énonce sont applicables au vote électronique tel qu'elle le définit. Les systèmes annexes, qui sont liés au vote électronique mais qui, techniquement parlant, n'en font pas partie, comme les systèmes d'enregistrement des électeurs, exigent une réglementation spécifique. Les présentes normes relatives au vote électronique peuvent être une source d'inspiration pour ce type de réglementation. Les États membres qui envisagent d'introduire le vote électronique peuvent aussi étudier le manuel sur le vote électronique du Conseil de l'Europe, qui peut les aider et les orienter concernant la mise en œuvre de ce mode de vote (*E-voting Handbook - Key steps in the implementation of e-enabled elections*, 2010).

11. Les nouvelles « Lignes directrices pour la mise en œuvre des dispositions de la Recommandation Rec(2017)5 sur les normes relatives au vote électronique » qui accompagnent la présente recommandation donnent des consignes détaillées pour atteindre les objectifs (fixés dans les normes). Elles incluent une version actualisée des dispositions qui figuraient dans l'ancienne Recommandation Rec(2004)11 et dans les deux séries de lignes directrices qui lui sont associées, à savoir les « Lignes directrices pour la conception de processus de confirmation du respect des exigences et normes recommandées (certification des systèmes de vote électronique) » et les « Lignes directrices relatives à la transparence des élections par voie électronique ». Les nouvelles Lignes directrices remplacent ces deux précédents textes.

[1] La Commission européenne pour la démocratie par le droit (Commission de Venise) a publié un « Rapport sur la compatibilité du vote à distance et du vote électronique avec les standards du Conseil de l'Europe » (adopté lors de sa 58e session plénière, Venise, 12-13 mars 2004, Etude n° 260/2003, Strasbourg, 18 mars 2004, CDL-AD(2004)012). Dans ses conclusions, elle estime que le vote à distance est compatible avec les normes du Conseil de l'Europe à condition que certaines mesures préventives soient respectées dans la procédure soit du vote par correspondance, soit du vote électronique.

12. La version actuelle des Lignes directrices doit être complétée par la poursuite des efforts visant à tenir compte de toutes les formes et tous les aspects de vote électronique couverts par la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique. Par ailleurs, au vu des évolutions permanentes dans les domaines juridique et technique, leurs dispositions devront être mises à jour régulièrement, tandis que la recommandation a vocation à créer un cadre stable. La mise à jour des Lignes directrices sera envisagée et décidée par les États membres lors des réunions périodiques destinées à faire le point sur la mise en œuvre de la présente recommandation.

Recommandations

13. On ne peut concevoir la démocratie sans élection ou référendum organisé(e) dans le respect de certains principes qui leur confèrent un caractère démocratique. Ces principes constituent un aspect spécifique du « patrimoine constitutionnel européen », qu'on appelle aussi « patrimoine électoral européen ». En 2002, la Commission européenne pour la démocratie par le droit (Commission de Venise) a adopté le Code de bonne conduite en matière électorale[2]. Ce texte, bien que non contraignant, est le document de référence du Conseil de l'Europe dans ce domaine. Il définit le « patrimoine électoral européen » par deux aspects : le noyau dur des principes constitutionnels du droit électoral et un certain nombre de conditions de base nécessaires à leur application. Le Code identifie les principes suivants : un suffrage universel, égal, libre, secret et direct, et des élections périodiques. Les conditions de base sont la primauté du droit, le respect des droits fondamentaux, la stabilité du droit électoral et des garanties procédurales effectives[3]. Tous les modes de suffrage utilisés lors des élections et des référendums, y compris le vote électronique, doivent être conçus et mis en œuvre dans le respect de ces principes et conditions.

14. Sur la base du Code de bonne conduite en matière électorale de 2002, les principes et conditions peuvent être résumés comme suit :

- *suffrage universel :* tout individu a le droit de vote et d'éligibilité, sous réserve de certaines conditions, telles que son âge et sa nationalité ;
- *suffrage égal :* tous les électeurs ont le même nombre de voix, chaque voix a le même poids et l'égalité des possibilités doit être garantie ;
- *suffrage libre :* l'électeur a le droit de former et d'exprimer librement son opinion, sans être soumis à une contrainte ou à une influence indue ;
- *suffrage secret :* l'électeur a le droit de voter dans le secret, à titre individuel, et l'État a le devoir de protéger ce droit ;
- *suffrage direct :* les suffrages des électeurs déterminent directement la ou les personnes élues ;
- *périodicité des élections :* des élections doivent être organisées à intervalles réguliers ;
- *respect des droits fondamentaux :* les élections démocratiques exigent le respect des droits de l'homme, comme la liberté d'expression, la liberté de circulation, la liberté de réunion et la liberté d'association ;
- *niveaux normatifs et stabilité du droit électoral :* les règles du droit électoral doivent avoir au moins rang législatif ; les règles techniques et de détail peuvent avoir un caractère réglementaire. Les éléments fondamentaux du droit électoral ne devraient pas pouvoir être modifiés moins d'un an avant une élection, ou devraient être traités au niveau constitutionnel ou à un niveau supérieur à celui de la loi ordinaire ;
- *garanties procédurales :* elles visent notamment à assurer l'organisation des élections par un organe impartial, l'observation des scrutins par des observateurs nationaux et internationaux, et l'existence d'un système de recours efficace ;
- *système électoral :* le choix du système électoral est libre, sous réserve du respect des principes mentionnés ci-dessus.

15. Les normes figurant dans l'annexe I de la recommandation fixent des objectifs que le vote électronique doit permettre d'atteindre pour respecter les principes et conditions du « patrimoine électoral européen ». Cependant, tous les principes et conditions mentionnés n'appellent pas une attention particulière et la fixation d'objectifs propres au vote électronique. C'est, par exemple, le cas des « élections périodiques » : ce principe n'exige pas une attention particulière lors de la conception ou de la mise en

[2] Le Code de bonne conduite en matière électorale (CDL-AD(2002)023rev), approuvé par la Résolution 1320 (2003) de l'Assemblée parlementaire et la Résolution 148 (2003) du Congrès des pouvoirs locaux et régionaux, a fait l'objet d'une Déclaration du Comité des Ministres (114e session, 13 mai 2004).

[3] - Le point 7 du Document de la réunion de Copenhague de la Conférence sur la dimension humaine de la CSCE du 29 juin 1990 parle clairement de suffrage libre, universel, égal et secret ; le point 6 mentionne le suffrage direct, quoique sous une forme nuancée.
- L'article 25(b) du Pacte international relatif aux droits civils et politiques prévoit expressément tous ces principes, sauf celui du suffrage direct, qui lui est implicite (article 21 de la Déclaration universelle des droits de l'homme).
- L'article 3 du Protocole additionnel à la Convention européenne des droits de l'homme prévoit expressément le droit à des élections libres au scrutin secret, organisées à des intervalles raisonnables ; les autres principes sont également reconnus par la jurisprudence en matière de droits de l'homme (caractère universel : CEDH n° 9267/81, arrêt dans l'affaire Mathieu-Mohin et Clerfayt c. Belgique, 2 mars 1987, Série A vol. 113, p. 23 ; arrêt dans l'affaire Gitonas et autres c. Grèce, 1er juillet 1997, nos 18747/91, 19376/92, 19379/92, 28208/95 et 27755/95, Recueil des arrêts et décisions, 1997-IV, p. 1233 ; égalité : arrêt précité dans l'affaire Mathieu-Mohin et Clerfayt c. Belgique, p. 23). Le droit à des élections au suffrage direct a été implicitement admis par la Cour de Strasbourg (CEDH n° 24833/94, arrêt dans l'affaire Matthews contre Royaume-Uni, 18 février 1999, Recueil des arrêts et décisions, 1999-I, para. 64.)

œuvre du vote électronique, si ce n'est, bien évidemment, que les modes de suffrage (y compris le vote électronique) devraient permettre l'organisation d'élections périodiques. Les normes énoncées dans la recommandation traitent exclusivement les questions concernant spécifiquement le vote électronique.

Point I : recommandations *i* à *vi*

Recommandations i et *ii. : Respect des principes et politique des risques*

16. Le vote électronique, comme tout mode de suffrage, doit respecter les principes des élections et référendums démocratiques. L'évolution rapide de la technologie sous-jacente représente un défi en la matière, car elle ne cesse de faire apparaître de nouvelles possibilités et menaces, qu'il convient de gérer comme il faut. Au final, il est essentiel que les solutions électroniques introduites dans les procédures de vote et/ou de dépouillement, ou leur évolution, ne portent pas atteinte à ces principes.

17. En conséquence, les systèmes de vote électronique doivent être conçus et utilisés de manière à garantir en permanence le respect des principes. Les États membres devraient accorder une attention particulière aux risques inhérents à la méthode retenue en matière de vote électronique. Ces risques doivent faire l'objet d'un contrôle en continu, donnant lieu si nécessaire à des mesures appropriées pour remédier aux problèmes. Compte tenu de la rapidité des changements dans le domaine des nouvelles technologies, il est conseillé aux États membres de mettre en place un cadre politique de gestion des risques.

18. Les principes peuvent souffrir des exceptions, et des restrictions concernant les conditions de mise en œuvre de ces principes peuvent s'appliquer. De plus, dans un contexte de vote électronique, il peut être nécessaire d'appliquer plus strictement tel principe et plus souplement tel autre. Ces décisions sont adoptées par l'autorité nationale compétente (Parlement, juge de la Cour suprême, administration électorale ou autorité gouvernementale) et dépendent du contexte propre au pays. Il est important que ce type de décision soit conforme aux exigences fondamentales, c'est-à-dire qu'elle soit adoptée par l'autorité compétente, qu'elle trouve son fondement dans la loi, qu'elle présente un intérêt général et qu'elle respecte le principe de proportionnalité, entre autres. Il est impératif de respecter l'objectif général des élections et référendums démocratiques.

19. Les principes régissant les élections démocratiques auxquels se réfère la recommandation sont ceux du patrimoine électoral européen figurant dans le Code de bonne conduite en matière électorale de la Commission de Venise. Ils constituent des exigences minimales et s'appliquent dans toute la région. Un pays peut adopter des principes supplémentaires ou opter pour une interprétation plus stricte des principes présentés ici. Dans ce cas, le vote électronique devra respecter des principes et normes qui sont plus strictes que ceux énoncés dans la présente recommandation.

Recommandation iii. :Orientations formulées dans la recommandation en matière d'examen de la législation interne, Articulation entre l'annexe I et les Lignes directrices

20. Le respect des principes est garanti de différentes manières et par différents moyens, selon le mode de suffrage et la technologie sous-jacente. Les normes figurant dans l'annexe I à la recommandation traduisent les principes en objectifs concrets. Les Lignes directrices donnent des orientations sur la mise en œuvre des objectifs. Il est prévu qu'elles soient régulièrement complétées et mises à jour à l'avenir, de manière à suivre le rythme des expériences pratiques et de l'évolution des nouvelles technologies.

21. Il existe un lien étroit entre la nouvelle recommandation et les nouvelles Lignes directrices. L'annexe I à la recommandation contient des normes élevées, qui constituent un noyau dur et fixent des objectifs que le vote électronique doit permettre d'atteindre pour respecter les principes des élections démocratiques. Ces normes devraient être stables dans le temps. Les Lignes directrices renferment des dispositions détaillées relatives à la mise en œuvre de ces objectifs (normes). Elles sont basées sur les expériences faites par les États membres, les développements intervenus sur leur territoire et les suggestions émanant des chercheurs universitaires.

22. Il est préconisé que les États membres se guident, dans leur législation, sur les normes énoncées à l'annexe I de la recommandation, quand ils optent pour le vote électronique. Une attention particulière doit être accordée à certains aspects juridiques au-delà du matériel électronique nécessaire et de son utilisation. L'ampleur de l'examen opportun dépendra des lois en vigueur dans l'État membre en question. On peut citer, entre autres exemples, les dispositions propres aux méthodes de vote, la législation pénale relative aux questions électorales, la législation sur la protection des données ou la législation en matière d'observation des élections.

23. Il est recommandé aux États membres de réfléchir aux autres modifications législatives qui peuvent s'avérer nécessaires suite à l'introduction du vote électronique.

Recommandations iv et v : Examen de la mise en œuvre et politique d'actualisation sur la base du partage d'expériences en la matière

24. Le vote électronique est un nouveau domaine qui se développe rapidement. Les normes et les lignes directrices doivent évoluer avec les nouveautés juridiques et techniques. Partant, il est recommandé à chaque État membre de suivre l'évolution de sa propre situation concernant le vote électronique, de faire état au Conseil de l'Europe des résultats de cet examen et de participer aux travaux d'actualisation de la recommandation et des Lignes directrices (voir Point II). Le Conseil évaluera la mise en œuvre de la recommandation au moins tous les deux ans après son adoption et les États membres échangeront sur leur expérience en la matière.

Recommandation vi. : Traduction et diffusion

25. La recommandation et les Lignes directrices qui l'accompagnent devraient être traduites et diffusées dans la langue locale par chaque État membre afin d'informer de manière adéquate les administrations électorales, les responsables électoraux, les citoyens, les partis politiques, les observateurs nationaux et internationaux, les ONG, les médias, les universitaires, les fournisseurs de solutions de vote électronique et les organismes de contrôle des systèmes de vote électronique.

Point II : Actualisation des Lignes directrices

26. Les Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique sont un document évolutif et devraient être actualisées régulièrement dès lors que les nouveautés juridiques, opérationnelles ou techniques l'imposent. L'examen susmentionné (paragraphe 24) permettrait d'évaluer cette nécessité.

Point III : Abrogation de la Rec(2004)11 du Comité des Ministres

27. La nouvelle Recommandation CM/Rec(2017)5 du Comité des Ministres aux États membres sur les normes relatives au vote électronique et les Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 annulera et remplacera la Recommandation Rec(2004)11 du Comité des Ministres aux États membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique et les Lignes directrices pour la conception de processus de confirmation du respect des exigences et normes recommandées (certification des systèmes de vote électronique) ainsi que les Lignes directrices relatives à la transparence des élections par voie électronique. Cela évitera toute confusion quant aux principes, normes ou Lignes directrices désormais applicables au vote électronique dans les États membres du Conseil de l'Europe.

Normes

28. L'annexe I à la recommandation contient une série de normes relatives au vote électronique qui fixent des objectifs que le vote électronique doit permettre d'atteindre pour respecter les principes régissant les élections et référendums démocratiques. Il s'agit de normes minimales qui, appliquées au système de vote électronique, faciliteraient le respect des principes régissant les élections et référendums démocratiques, sans toutefois que cette mise en œuvre constitue à elle seule un gage de qualité démocratique. La législation nationale peut ainsi prévoir des exigences supplémentaires. L'évaluation du vote électronique lors d'une élection ou d'un référendum doit se fonder sur un examen approfondi de la procédure dans son ensemble, en tenant compte du contexte, mais le respect des normes est un élément important pour améliorer la qualité démocratique du système de vote électronique.

Définitions interprétatives

29. L'annexe II qui figure à la fin du document comporte les définitions des termes utilisés dans la recommandation, son annexe I et le présent exposé des motifs. Il conviendrait de se référer à ces définitions lors de la traduction de tout ou partie de la recommandation dans d'autres langues.

ANNEXE I : NORMES RELATIVES AU VOTE ÉLECTRONIQUE

SUFFRAGE UNIVERSEL

Norme n° 1. « L'interface utilisateur du système de vote électronique sera... »

30. Pour respecter le suffrage universel, les États membres doivent faire en sorte que l'interface électeur du système de vote électronique soit compréhensible et utilisable par le plus grand nombre d'électeurs possible. Il faut réfléchir à l'ergonomie lors de la conception de l'interface de vote électronique, afin de tenir compte de l'interaction entre celle-ci et l'électeur. L'objectif est que l'électeur puisse utiliser facilement le système et suivre les instructions, y compris celles qui ont trait à la sécurité.

31. Il faut aussi prendre en considération les différentes contraintes liées à l'utilisateur (âge, langue, mode de vie, etc.). Les instructions données aux électeurs doivent être claires et faciles à comprendre et à suivre par le plus grand nombre.

Norme n° 2. « Le système de vote électronique sera, dans toute la mesure du possible, conçu… »

32. Certaines personnes handicapées ne sont pas en mesure d'utiliser le vote électronique. La conception du système de vote électronique devrait toutefois viser à exploiter toutes les possibilités d'accessibilité qui sont offertes aux personnes handicapées. Combiné aux autres modes de suffrage existants, le vote électronique a pour objet de permettre au plus grand nombre de personnes handicapées et de personnes ayant des besoins spéciaux de voter de façon autonome.

33. Au niveau de la mise en œuvre, l'autorité compétente décide de la manière de répondre aux besoins des personnes handicapées et des personnes ayant des besoins spéciaux. Ainsi, les personnes souffrant de troubles de la vue ou de dyslexie apprécieront des dispositifs de lecture d'écran, un fort contraste entre le texte et le fond, ainsi que la possibilité d'ajuster la taille du texte dans leur navigateur internet ou dans la machine de vote. Les utilisateurs atteints de troubles de la communication pourront préférer des informations présentées de manière graphique. Ceux qui ont des troubles de la coordination préféreront le clavier à la souris. Les interfaces de vote doivent être adaptées aux besoins des personnes à mobilité réduite.

34. Les solutions adaptées aux personnes handicapées peuvent être plus vulnérables aux menaces pour la sécurité du vote électronique. C'est pourquoi il appartient à l'autorité compétente de décider de les développer et de les utiliser dans la mesure du possible, c'est-à-dire en trouvant un équilibre acceptable entre la capacité effective d'utilisation et la sécurité.

Norme n° 3. « À moins que les modes de vote électronique à distance ne soient universellement accessibles... »

35. La mise en place de modes de suffrage supplémentaires, en l'occurrence le vote électronique, s'ajoutant aux modes de vote traditionnels peut rendre les élections et les référendums plus accessibles et renforcer ainsi le principe d'universalité. À l'inverse, le fait de proposer uniquement un mode de vote électronique à distance restreint l'accessibilité, car internet n'est pas disponible partout à l'heure actuelle. Cette disposition vise à protéger les électeurs, afin que le mode de suffrage qui leur est offert soit effectivement accessible.

Norme n° 4. « Avant d'enregistrer un suffrage utilisant un système de vote électronique à distance, l'attention des électeurs… »

36. Lorsque des modes de suffrage totalement nouveaux sont mis en place, en particulier le vote électronique à distance, il convient d'attirer l'attention des électeurs sur le fait que ce système est officiel et qu'il est utilisé dans une élection ou un référendum réels. L'objectif est d'éviter que les électeurs aient l'impression de participer à une élection ou un référendum factice ou à un test. Les mêmes efforts de communication devraient être faits lorsque les personnes utilisent une version de démonstration ou de test, afin qu'elles ne s'imaginent pas avoir réellement voté. En outre, il faudrait clairement distinguer les élections et les référendums des sondages, et vice versa.

SUFFRAGE ÉGAL

Norme n° 5. « Toutes les informations officielles relatives au scrutin seront présentées... »

37. Toutes les informations officielles relatives au scrutin, en particulier les options de vote, seront présentées de manière égale pour l'ensemble des modes de suffrage. Cela implique une égalité de contenu. Il conviendrait d'adopter des mesures pour prévenir d'une part l'omission d'informations qui devraient apparaître sur le bulletin électronique et d'autre part la diffusion de toute information autre que celles qui doivent figurer sur le bulletin officiel selon la loi.

38. Cela implique également qu'il doit y avoir une égalité quant à l'affichage de l'information. Cependant, il peut être difficile voire impossible de parvenir à une égalité totale, car les différents supports (téléphones portables, téléviseurs numériques, machines de vote électronique ou ordinateurs) affichent les informations de différentes façons à l'écran. Dans ce cas, il faudrait reconnaître qu'il ne s'agit pas d'une question purement technique et que la décision ne devrait pas être laissée au seul personnel technique. L'administration électorale devrait fournir des orientations en la matière.

Norme n° 6. « Lorsque des modes de vote électroniques et non électroniques sont utilisés... »

39. Les votes électroniques sont tout d'abord décryptés et comptabilisés. Les résultats sont ensuite ajoutés à ceux obtenus avec les bulletins papier, puis le résultat final est calculé. Pour ce faire, une méthode d'agrégation, probablement un logiciel, est nécessaire. Elle doit répondre aux mêmes objectifs de sécurité et de fiabilité que le logiciel de vote électronique.

40. Lorsque le nombre de votes électroniques ou de bulletins sur papier est particulièrement faible, il y a un risque que le secret du scrutin soit violé si les résultats de ces rares suffrages sont divulgués. La méthode d'agrégation devrait présenter les garanties techniques et procédurales nécessaires pour permettre la consolidation des résultats des différents modes de suffrage avant la divulgation des résultats, ce qui préserverait le secret du scrutin. En outre, les règles procédurales, notamment celles qui portent sur le personnel intervenant dans le processus de dépouillement, devraient tenir compte de ce type de cas.

Norme n° 7. « L'identification exclusive des électeurs... »

41. L'identification exclusive désigne la validation de l'identité d'une personne donnée grâce à une ou plusieurs caractéristiques permettant à coup sûr de la distinguer de toute autre. Les listes électorales devraient donc fournir le moyen d'éviter les doublons numériques – c'est-à-dire que les mêmes données d'identification soient attribuées à plusieurs personnes. Dans le cas de listes électorales centralisées, l'identification exclusive peut implicitement être assurée par l'inscription de la personne dans la base de données. Quand le système utilise des listes électorales fédérées, des moyens supplémentaires peuvent être nécessaires.

42. Une personne pouvant être à la fois électeur et candidat, il est important d'éviter qu'elle dispose des mêmes données d'identification pour tous ses rôles. Il en va de même pour les personnes qui peuvent être à la fois administrateur du système de vote électronique et électeur. L'authentification peut être basée sur l'identité ou sur le rôle. Le premier cas est conseillé pour les électeurs qui enregistrent ou qui expriment un vote, ou pour la nomination d'un candidat. L'authentification basée sur le rôle peut être suffisante pour les administrateurs, les contrôleurs, etc.

Norme n° 8. « Le système de vote électronique n'autorisera l'accès d'un utilisateur... »

43. Quand des jetons anonymes de vote attestent le droit de vote d'un électeur, l'authentification de ce dernier peut être facultative à ce stade, car elle a déjà eu lieu précédemment (lorsqu'un jeton précis est attribué à un électeur précis).

Norme n° 9. « Le système de vote électronique fera en sorte que seul le nombre approprié de suffrages... »

44. Il faudrait compter l'ensemble des votes, qu'ils soient exprimés par voie électronique ou traditionnelle, et s'assurer que seuls les suffrages d'électeurs habilités ont été pris en compte dans le résultat de l'élection. Le principe « une personne, une voix » sera respecté et seul le nombre approprié de suffrages, prévu dans la législation, est alloué à chaque électeur.

SUFFRAGE LIBRE

Norme n° 10. « L'intention de l'électeur ne sera pas affectée... »

45. Le système de vote ne doit pas influer sur les intentions de vote des électeurs habilités. L'exercice personnel du droit de vote est un principe fondamental. Une attention particulière est accordée à ce point, très sensible dans le cadre du vote électronique à distance. La norme susmentionnée n'interdit pas le vote électronique à distance. En revanche, des dispositions adéquates devraient être adoptées aux niveaux de la réglementation et de la mise en œuvre pour garantir le respect du suffrage personnel et libre. Il en va de même pour le vote électronique local.

46. Dans un environnement de vote électronique à distance, il faut envisager, entre autres éventualités, l'imitation d'un serveur officiel par manipulation du système de nom de domaine (DNS), l'utilisation d'un nom de domaine similaire à celui du serveur officiel de vote électronique, une attaque de type « man-in-the-middle », ou un logiciel malveillant dans le système de l'électeur qui remplace le bulletin original ou envoie de faux bulletins.

47. Selon les lois et politiques nationales, et dans un souci d'accessibilité, le principe d'universalité peut primer sur le principe du suffrage personnel ; c'est pourquoi, par exemple, le vote par procuration peut être autorisé. Il en va de même pour le mode de vote par voie électronique. Cependant, là encore, les règles et conditions régissant le vote par procuration seront respectées.

48. Les signatures électroniques, les codes de contrôle ou les autres techniques appliquées au bulletin peuvent permettre de vérifier que le suffrage n'a pas été manipulé. Le recours à ces techniques doit toutefois respecter le secret du scrutin. Dans le même temps, il conviendrait de prévoir clairement la marche à suivre dans l'hypothèse où la vérification ferait apparaître une manipulation du vote.

Norme n° 11. « On garantira que le système de vote électronique présente un bulletin authentique... »

49. Outre les techniques prévues aux normes 5 et 10, la norme 11 exige d'adopter des mesures procédurales pour s'assurer que toutes les informations indiquées dans le système de vote électronique et présentées à l'électeur via l'interface de vote électronique sont authentiques, c'est-à-dire identiques à celles fournies par l'autorité compétente.

Norme n° 12. « La manière dont les électeurs sont guidés... »

50. Pendant le déroulement du vote, il est important que les décisions ne puissent être prises en appuyant par inadvertance sur un bouton ou en cliquant par erreur sur un lien, et qu'elles reflètent véritablement la volonté de l'électeur. Ce dernier devrait se voir rappeler au début de la procédure qu'il prend part à un vote réel, surtout lorsque le vote électronique a lieu depuis un environnement non contrôlé. Tout au long de la procédure, qu'il s'agisse de cadres de vote électronique contrôlés ou non, l'électeur devrait disposer d'un temps suffisant pour réfléchir et réagir, de telle sorte qu'il ne soit pas obligé de voter sans réfléchir aux choix qu'il indique. La conception de l'interface, les messages donnés à l'électeur et tout autre aspect pertinent devraient être programmés pour permettre à l'électeur d'exprimer sa véritable volonté. À la fin de la procédure de vote, après un résumé de ses choix, l'électeur est invité à confirmer que ce résumé reflète sa véritable volonté. C'est seulement après cette étape que le vote est envoyé au serveur de vote ou placé dans l'urne électronique. La mise en œuvre détaillée de cette disposition peut toutefois varier selon les spécificités du système de vote électronique utilisé.

Norme n° 13. « Le système de vote électronique offrira à l'électeur... »

51. Dans les systèmes de vote avec bulletins sur papier, les électeurs ont la possibilité de participer à l'élection mais sans pour autant exprimer une préférence parmi les choix proposés. La norme ci-dessus établit que cette possibilité doit être maintenue dans le cadre du vote électronique.

52. Cette norme n'influe pas sur la validité ou les effets juridiques d'un vote blanc ou d'un vote intentionnellement nul. Ces questions sont réglementées au niveau national. Les pays décident, par exemple, si ces votes sont acceptés, comment ils sont comptabilisés (s'ils le sont) ou quel est leur effet juridique sur le résultat. Dès lors que le « vote blanc » est déjà prévu sur le bulletin, il suffit que cette option figure aussi sur le bulletin électronique. Cette norme interdit simplement un système dans lequel l'électeur serait obligé de sélectionner un choix (autre que le vote blanc) pour terminer la procédure de vote. Ce faisant, l'objectif est d'offrir des garanties identiques à celles des systèmes de vote avec bulletins sur papier, où l'électeur a le choix de ne choisir aucun des candidats proposés, par exemple.

Norme n° 14. « Le système de vote électronique avisera l'électeur... »

53. Comme expliqué aux précédents paragraphes, la recommandation n'empêche pas les États membres de proposer d'autres options de vote, comme la possibilité d'exprimer intentionnellement un vote nul. De plus, des suffrages exprimés dans le but d'être valables peuvent, dans des circonstances bien précises, être invalidés en raison de complications techniques, par exemple, sans que l'électeur en soit nécessairement conscient. La norme ci-dessus n'impose pas de prévoir la possibilité du vote nul parmi les options de vote. Elle exige seulement que lorsqu'un vote nul est reçu par le système de vote électronique, quelle qu'en soit la raison, l'électeur ayant exprimé ce vote en soit informé. L'objectif est d'éviter les votes qui ne soient pas intentionnellement nuls. Cela vaut pour tous les cas, que le système de vote électronique autorise ou non les votes nuls. Naturellement, cela ne s'applique qu'aux votes exprimés par voie électronique.

54. Lorsqu'il informe l'électeur que son vote est nul, le système devrait également l'informer des conséquences de cette nullité (est-elle prise en compte ou non ? etc.) et de la possibilité de revoter si la nullité n'était pas intentionnelle. Si le système n'accepte pas les votes nuls, le bulletin peut être refusé, ou admis puis écarté. Si le système accepte les votes nuls, le bulletin sera accepté en attendant la réaction de l'électeur : si la nullité n'était pas intentionnelle, l'électeur pourrait souhaiter revoter ; dans le cas contraire, il a exprimé un vote intentionnellement nul et maintient son choix. Presque tout dépend dans ce cas de la réglementation nationale concernant les votes nuls. L'avantage d'un système de vote électronique est qu'il est possible d'informer l'électeur, qui peut alors réagir si le vote nul ne reflète pas son véritable choix.

Norme n° 15. « L'électeur devra pouvoir vérifier que... »

55. Les normes 15 à 18 introduisent des mécanismes de contrôle qui développent le concept de chaîne de confiance dans les élections par voie électronique. La norme 15 fait référence aux outils de contrôle qui permettent à l'électeur de vérifier que son vote a été exprimé comme il le souhaitait et enregistré comme tel, ce que l'on appelle également la vérifiabilité individuelle. Les outils de vérifiabilité individuelle varient selon la solution de vote électronique déterminée. Le reçu papier édité à l'issue du vote par la machine de vote électronique utilisée dans un bureau de vote ou les codes retour utilisés dans le cadre du vote par internet en sont des exemples.

56. La norme 16 porte sur la confirmation par le système que la procédure de vote s'est achevée avec succès. La norme 17 a trait aux outils de contrôle qui permettent à toute personne intéressée de vérifier que les votes sont comptabilisés tels qu'ils ont été enregistrés (vérifiabilité universelle) et la norme 18 dispose qu'il est possible de vérifier que seuls les votes des électeurs habilités ont été pris en compte dans le résultat final, ce qui boucle la boucle de la chaîne de confiance.

Norme n° 16. « L'électeur recevra la confirmation... »

57. La procédure de vote est achevée avec succès lorsque le bulletin électronique est déposé dans l'urne électronique. Dans le cadre du vote électronique à distance, cela signifie que la procédure de vote ne se termine qu'après que le bulletin est parvenu à destination, c'est-à-dire après son envoi depuis le dispositif de vote de l'électeur (ordinateur, téléphone, etc.), par internet ou par un autre réseau, vers le serveur faisant office d'urne électronique.

58. Le système confirme à l'électeur que son bulletin est déposé dans l'urne et sera comptabilisé et que la procédure de vote s'est achevée avec succès. Dès l'instant où l'électeur en est informé, il peut se déconnecter en toute sécurité ou interrompre la connexion. Les deux messages (sur le dépôt du bulletin et l'achèvement de la procédure) peuvent être réunis en un seul si les deux moments coïncident. Une bonne pratique consiste à accompagner ces messages d'un rappel et d'instructions indiquant à l'électeur comment effacer les traces de son vote si le scrutin a eu lieu depuis un dispositif non contrôlé.

Norme n° 17. « Le système de vote électronique produira des preuves tangibles que chaque suffrage authentique... »

59. Le système de vote garantit que chaque suffrage est correctement inclus dans les résultats des élections. Cela suppose la capacité de fournir des preuves fiables aux électeurs et aux tiers pour leur prouver que les résultats représentent véritablement et précisément les suffrages authentiques exprimés et répondent aux exigences de la réglementation applicable aux élections et référendums démocratiques. Les « preuves fiables » renvoient aux critères à respecter pour que ces preuves soient largement acceptées. Les « suffrages authentiques » renvoient aux normes mentionnées plus haut qui garantissent que le vote reflète la libre volonté de l'électeur.

60. En outre, il devrait être possible de contrôler les preuves pour vérifier leur exactitude à l'aide d'outils distincts et indépendants du système de vote électronique. Pour ce faire, le système de vote électronique devrait proposer des interfaces dotées de possibilités d'observation et de contrôle élaborées, dans les limites imposées par le secret et l'anonymat du vote.

61. Le pourcentage de votes exprimés par voie électronique et la comparaison des résultats du vote électronique avec les résultats du vote par d'autres modes de suffrage peuvent être pris en compte pour contrôler la vraisemblance des résultats du vote électronique et valider ainsi leur exactitude.

Norme n° 18. « Le système produira des preuves tangibles que seuls les suffrages d'électeurs habilités... »

62. Les électeurs et les tiers devraient pouvoir vérifier que seuls les votes des électeurs habilités ont été pris en compte dans le résultat de l'élection. Dans le même temps, les suffrages comptabilisés devraient être anonymes. Dans le cas du vote par internet, il existe des méthodes de cryptage avec lesquelles il n'est pas nécessaire de procéder au décodage avant le dépouillement (cryptage homomorphique). Le dépouillement peut intervenir sans que soit révélé le contenu des suffrages cryptés.

SUFFRAGE SECRET

Norme n° 19. « Le vote électronique sera organisé de manière à... »

63. Cette norme pose le principe général du secret du vote, applicable à la procédure tout entière, laquelle recouvre la période préélectorale (communication aux électeurs des numéros d'identification personnels ou des jetons électroniques), le remplissage et l'envoi du bulletin ainsi que le comptage et le recomptage des suffrages.

64. Les mesures à prendre incluent naturellement le cryptage, mais aussi, par exemple, le fait de mélanger les suffrages exprimés dans l'urne électronique, afin que l'ordre dans lequel ils apparaissent lors du dépouillement ne permette pas de déduire l'ordre de leur arrivée.

Norme n° 20. « Le système de vote électronique ne traitera et ne stockera... »

65. Le système de vote ne traitera et stockera que les données à caractère personnel sans lesquelles il ne peut fonctionner correctement. Cette exigence, également appelée « limitation des données », fait référence aux données nécessaires pour satisfaire aux obligations juridiques de la procédure de vote. L'administration électorale chargée de l'organisation du vote électronique identifie ces données et devrait être en mesure d'expliquer quelles sont les dispositions et considérations juridiques sous-jacentes qui les rendent indispensables. La durée du traitement, du stockage, etc. dépend aussi des obligations juridiques, par exemple celles qui concernent les recours. La limitation des données vise à garantir la protection des données et fait partie du secret du scrutin.

Norme n° 21. « Le système de vote électronique et toute partie autorisée… »

66. Le droit interne peut prévoir différents moyens d'identification et d'authentification pour les différents modes de suffrage (indication du nom de l'électeur, présentation d'une carte d'identité, utilisation de codes propres à chaque électeur, etc.). L'objectif général est de faire en sorte que seules les personnes ayant le droit de voter puissent effectivement voter, et d'empêcher les suffrages multiples et autres infractions.

67. Cette norme signifie que le système lui-même et toute partie autorisée ont entre les mains, à un moment donné, les informations d'authentification. Un exemple de partie autorisée est l'organisme qui imprime le matériel de vote contenant les informations d'authentification. Le système et toute partie autorisée devraient protéger ces informations par des moyens techniques et organisationnels. Toute autre personne, par définition non autorisée, ne devrait en aucun cas pouvoir accéder à ces données ou les utiliser.

68. D'autres services, comme ceux qui informent les électeurs avant le début de la procédure de vote, pour lesquels l'authentification est évidemment sans objet, sortent du cadre de la présente norme.

Norme n° 22. « Les listes électorales enregistrées ou communiquées par le système de vote électronique... »

69. Cette norme dispose que seules les parties autorisées ont accès spécifiquement aux listes électorales.

Norme n° 23. « Le système de vote électronique ne fournira pas de preuve du contenu du suffrage enregistré à l'électeur... »

70. L'objectif de cette norme est d'empêcher la violation du secret du scrutin et la vente de voix. La vérifiabilité individuelle pourra néanmoins être mise en œuvre s'il existe des garanties appropriées contre la pratique de l'achat de voix ou l'exercice de pressions sur l'électeur.

71. Des dispositions régissant la violation du secret du scrutin ou la vente de voix devraient être en vigueur. Dans de nombreux pays, ces violations sont couvertes par le droit pénal. Les dispositions en question englobent tous les modes de suffrage utilisés et devraient aussi s'appliquer au vote électronique. Elles devraient être actualisées, si nécessaire, pour tenir compte des spécificités du vote électronique.

72. Lorsqu'une preuve écrite du contenu du vote est présentée, comme c'est le cas dans les environnements contrôlés où des machines de vote électronique sont utilisées, des mesures techniques et organisationnelles devraient être en place pour empêcher l'électeur de faire de cette preuve un usage autre que l'usage normal prévu durant la procédure de vote. L'électeur ne peut, par exemple, utiliser la preuve pour violer le secret du vote ou l'emporter en dehors du cadre supervisé.

73. Dans un système de vote électronique à distance basé sur internet, l'électeur devrait être informé de la nécessité d'effacer les traces de l'opération de vote de l'appareil utilisé pour enregistrer son suffrage, ainsi que de la procédure à suivre. Des traces peuvent être conservées, par exemple, dans la mémoire de l'ordinateur personnel, dans le cache du navigateur, dans la mémoire vidéo, dans les fichiers d'échange (swap), dans les fichiers temporaires, etc.

74. Lors de la conception du système de vote électronique, il conviendrait d'être particulièrement attentif à la manière dont sont assurés l'anonymat et le secret du vote. En matière de vote électronique à distance, il faut prendre en considération au moins trois éléments : l'application web, le navigateur et le logiciel de travail sur l'ordinateur de l'électeur.

a. Au niveau de l'application web, il ne faudrait pas que l'utilisateur puisse conserver une copie de son vote. L'application ne devrait pas proposer les fonctions d'impression, de sauvegarde ou de stockage du vote ou (de la partie) de l'écran où le vote est visible.
b. De même, le navigateur ne devrait pas proposer d'option permettant d'imprimer l'écran sur lequel le vote est visible. Il conviendrait de noter que les logiciels de navigation peuvent conserver (et conservent) les informations de plusieurs manières. Par exemple, en utilisant le bouton « Précédent » du navigateur, on peut afficher un ou plusieurs écrans précédents. Cette fonctionnalité générique des navigateurs devrait être, autant que possible, désactivée par l'application web. À tout le moins, aucune information ne devrait être conservée après que l'électeur a envoyé son bulletin.
c. Il faut aussi tenir compte des logiciels qui peuvent enregistrer d'une façon ou d'une autre les opérations effectuées par tel utilisateur d'un ordinateur. Trois exemples assez répandus sont les logiciels de copie d'écran, les logiciels d'enregistrement des séquences d'écrans et les logiciels d'enregistrement des touches frappées par l'utilisateur. Ceux-ci peuvent être des logiciels malveillants, présents dans l'ordinateur de l'utilisateur sans que ce dernier en ait connaissance. Il se peut que le système de vote électronique n'ait pas la capacité d'empêcher cette présence. L'électeur devrait être informé de l'existence de ces logiciels malveillants, des risques potentiels qu'ils présentent, des bonnes pratiques à adopter pour réduire les risques le plus possible et, plus généralement, des autres modes de suffrage, plus sûrs, qui sont à sa disposition.

Norme n° 24. « Le système de vote électronique ne permettra pas de divulguer... »

75. Cette norme vise à empêcher l'établissement et la publication de résultats intermédiaires du vote électronique. Les informations sur les niveaux de participation ne relèvent pas de la présente norme et peuvent être réunies et diffusées comme le prévoit la réglementation nationale.

Norme n° 25. « Le vote électronique garantira que le secret des choix précédents... »

76. Cette norme exige que la confidentialité des précédents choix indiqués puis effacés par l'électeur au cours de la procédure de vote soit autant protégée que le secret du vote final.

Norme n° 26. « La procédure de vote électronique, en particulier au moment du décompte des voix... »

77. Cette norme énonce qu'il ne doit pas être possible d'établir un lien entre le vote et l'électeur. Elle prévient ainsi toute violation du secret du scrutin.

78. Dans une procédure de vote électronique local, l'identification de l'électeur et le vote peuvent être séparés physiquement, même lorsqu'un système de vote électronique est utilisé. Cette séparation physique peut, en principe, être contrôlée par le personnel chargé des élections et les observateurs des élections, à supposer qu'il y ait une erreur délibérée ou involontaire dans le système de vote électronique (mais pas de logiciel malveillant).

79. Dans la procédure de vote à distance, les informations liées à l'électeur (généralement un code) et les votes sont associés jusqu'à un certain stade. Dans les pays qui autorisent le vote multiple, ce lien est nécessaire pour gérer les différents votes et leurs effets (un vote en efface un autre). La séparation doit être faite par voie électronique à un stade prédéfini avant le dépouillement. Cela nécessite des solutions techniques spécifiques.

80. Lorsque le droit interne exige qu'il existe un lien permanent entre l'électeur et le vote, qui doit être maintenu tout au long de l'élection ou du référendum et pendant une durée précise par la suite, il faut s'assurer que ce lien est suffisamment protégé durant toute cette période afin de garantir le secret du scrutin. Le secret ne peut être levé que sur décision d'une juridiction compétente, en veillant à ce qu'aucun électeur ne soit contraint de révéler comment il a voté.

81. Un système de vérification devrait préserver à tout moment l'anonymat des électeurs, sauf quand la législation nationale prévoit spécifiquement le contraire. Les informations collectées par le système de vérification doivent toujours être protégées contre les accès non autorisés.

RÉGLEMENTATION ET ORGANISATION

Norme n° 27. « Les États membres qui mettent en place le vote électronique… »

82. Il conviendrait de mettre en place les technologies de vote électronique de manière graduelle et progressive et de les tester dans des conditions réalistes avant le jour du scrutin. D'après l'expérience acquise par les États membres, une mise en place progressive s'impose compte tenu des difficultés et des possibilités juridiques et techniques que présente le vote électronique. Certaines grandes étapes sont décrites dans les lignes directrices relatives à cette norme.

83. En particulier, l'introduction du vote électronique à distance ne pourrait se faire que si d'autres formes de vote à distance comme le vote par correspondance sont bien établies et éprouvées. Beaucoup de questions opérationnelles et liées à la confiance de l'utilisateur concernant le vote électronique à distance sont similaires à celles qui se posent pour le vote par correspondance et il est plus facile d'y répondre dans le contexte du vote par correspondance.

Norme n° 28. « Avant l'introduction du vote électronique, les États membres… »

84. Si cette norme peut sembler évidente à première vue, elle a pour objectif d'attirer l'attention des États membres sur le fait qu'en plus de définir les modalités du vote électronique, il se peut qu'ils doivent modifier la législation ou même la Constitution pour permettre le vote électronique. La législation en vigueur n'est pas conçue en tenant compte de l'automatisation et peut être ambigüe lorsqu'elle s'applique au vote électronique.

85. Autre enseignement tiré des expériences dans la région, les réglementations spécifiques au vote électronique doivent être détaillées pour permettre aux parties prenantes concernées de comprendre ce système et d'exercer leurs fonctions y afférentes, d'autant plus que cela permet de garantir que la mise en œuvre de ces technologies respecte les principes des élections et référendums démocratiques.

86. Le cadre juridique devrait prévoir un contrôle juridictionnel du vote électronique afin de permettre aux citoyens de remettre en question le mode de vote électronique effectivement utilisé, ainsi que sa mise en œuvre, renforçant par conséquent la confiance du public dans ce système.

Norme n° 29. « La législation pertinente réglementera les responsabilités… »

87. De nombreuses parties prenantes ont un rôle à jouer et une certaine responsabilité dans les processus de conception, de test, de certification, de mise en place, d'application, de maintenance, d'observation et de contrôle des systèmes de vote électronique. Mais, au final, l'État est globalement

responsable du vote et par conséquent du système de vote électronique. Il est recommandé que la législation pertinente prévoie la fonction de contrôle de l'administration électorale concernant le vote électronique. Le rôle et les responsabilités des autres parties impliquées devraient être précisés dans la réglementation ou le contrat approprié.

88. Afin de garantir le contrôle effectif de l'administration électorale sur le vote électronique, il est notamment important que les États membres ne confient pas cette tâche à un petit nombre de fournisseurs seulement, car cela pourrait entraîner une trop grande dépendance vis-à-vis de ces derniers. En effet, les logiciels et équipements utilisés pour le vote électronique nécessitent la mise en place d'une maintenance continue – procédure qui vient s'ajouter aux procédures à suivre pour tout événement électoral, telles que l'édition de bulletins papier. Dans les États qui envisagent la solution de l'externalisation, il est fondamental que les responsables électoraux aient connaissance des tâches qui seront externalisées et des raisons pour lesquelles elles le seront, ainsi que des méthodes et processus que le(s) fournisseur(s) entend(ent) appliquer. En revanche, au vu de l'importance de ses responsabilités, les obligations légales incombant à l'organe chargé de la conduite des élections ne doivent jamais être confiées à des tiers.

Norme n° 30. « Les éventuels observateurs pourront observer la comptabilisation des votes. L'administration électorale sera responsable du processus de dépouillement. »

89. L'objectif de cette norme est de souligner le rôle de l'administration électorale dans le processus de dépouillement, non seulement comme l'un des participants mais aussi en tant qu'organisateur et superviseur. Il conviendrait de prévoir la présence d'observateurs. Parmi eux devraient figurer des représentants des partis politiques ainsi que du public.

TRANSPARENCE ET OBSERVATION

Norme n° 31. « Les États membres feront preuve de transparence pour tous les aspects… »

90. L'instauration d'un système de vote électronique ne peut se faire qu'à condition que les électeurs aient pleinement confiance dans le système électoral et l'administration électorale en place. Toutefois, il ne faudrait jamais considérer cette confiance comme définitivement acquise et les États doivent s'efforcer au maximum de la préserver. Ainsi, pour favoriser la confiance de la population, il est fondamental d'encourager les États membres à faire preuve de transparence en ce qui concerne le système de vote électronique, les processus en la matière et les raisons qui sous-tendent l'introduction du vote électronique. Cette attitude devrait en effet permettre aux électeurs de mieux connaître et de comprendre la démarche adoptée par les États, et ainsi, susciter la confiance publique.

91. Cette norme exige une large transparence pour tous les aspects de toutes les formes de vote électronique. En particulier, la transparence du système, ou la possibilité de vérifier qu'il fonctionne correctement, doit être garantie. Les États membres définissent quelles parties prenantes ont accès à quels types d'informations, à quel moment, et dans quelles circonstances.

92. Par ailleurs, la transparence peut se traduire par une attitude d'ouverture au sujet de la procédure de vote électronique. Parallèlement au système de vote électronique, les États membres devraient aussi garantir la transparence de toutes les procédures (avant, pendant et après le jour du scrutin/la période électorale) liées au vote électronique, notamment par la publication d'illustrations (par exemple, photos, vidéos, etc.) sur le site officiel expliquant le vote électronique à l'ensemble des parties concernées. La langue des signes et le sous-titrage devraient également être utilisés afin que la communication sur le vote électronique touche un public aussi large que possible.

93. Il conviendrait de faire participer les représentants des personnes handicapées au processus d'introduction du vote électronique afin d'examiner les répercussions que ce nouveau mode électoral pourrait avoir pour les personnes qu'elles représentent.

Norme n° 32. « Le public, en particulier les électeurs, sera informé… »

94. Les procédures à suivre par les électeurs peuvent varier selon qu'il s'agit d'un mode de suffrage traditionnel ou électronique. Les différences portent, par exemple, sur la période pendant laquelle les votes peuvent être émis, la démarche que doit suivre l'électeur et le déroulement concret du vote. Elles devraient être communiquées aux électeurs afin de leur donner tous les éléments requis sur l'utilisation du mode de vote électronique et afin d'éviter tout malentendu concernant la procédure de vote. Il conviendrait de réfléchir au laps de temps nécessaire aux électeurs pour faire leur choix. Il faudrait penser également à donner aux utilisateurs la possibilité de vérifier la compatibilité de leur matériel avant de choisir un mode de suffrage.

Norme n° 33. « Les composantes du système de vote électronique seront divulguées… »

95. Il est essentiel de veiller à ce que les systèmes de vote électronique fonctionnent correctement et à ce que leur sécurité soit assurée. Cela se fait au moyen d'une certification ou d'une évaluation indépendante des éléments du système ou du système dans son ensemble, ce qui nécessite la divulgation de ses éléments critiques. L'évaluation peut être menée à bien de plusieurs manières : divulgation de la conception du système, examen d'une documentation détaillée, divulgation du code source, examen des rapports de certification et d'évaluation des éléments, tentatives d'intrusion avancées, etc. Le niveau de divulgation des éléments du système nécessaire à l'assurance de sa sécurité dépend des particularités, des éléments et des fonctions du système.

Norme n° 34. « Tous les observateurs devront pouvoir, dans les limites fixées par la loi… »

96. Si la mise à disposition des documents au public est importante, les électeurs ne sont pas tous en mesure de comprendre le fonctionnement d'un suffrage basé sur le vote électronique. La confiance de ces personnes repose sur d'autres parties prenantes qui ont les moyens de comprendre les matériels et processus en jeu. Par conséquent, il est fondamental que les observateurs aient un accès aussi large que possible aux réunions, activités et documents pertinents.

97. Il existe diverses obligations internationales et nationales en matière d'observation d'élections. Les observateurs devraient inclure des représentants des candidats et des partis politiques ainsi que le grand public et des observateurs indépendants nationaux et internationaux. Tous les États membres sont liés par le document de la réunion de Copenhague de la Conférence sur la dimension humaine de l'OSCE du 29 juin 1990, document dans lequel ils s'engagent à « inviter des observateurs de tout autre État participant à l'OSCE et de toute institution ou organisation privée compétente qui le souhaiterait, à suivre le déroulement de la procédure de leurs élections nationales […et…] à faciliter un accès analogue pour les élections organisées à un niveau inférieur au niveau national. » Les procédures d'acceptation des observateurs, ainsi que leurs droits et leurs obligations, sont définis par la législation du pays en la matière et devraient respecter les engagements internationaux du pays.

98. Les observateurs, dans les limites fixées par la loi, devraient pouvoir vérifier que le système de vote électronique, dans sa conception et son fonctionnement, respecte les principes fondamentaux des élections et référendums démocratiques. En conséquence, les États membres devraient mettre en œuvre des dispositions juridiques claires sur l'accès d'observateurs à la documentation concernant le système de vote électronique, y compris aux données résultats des audits.

99. Le vote électronique est porteur de problèmes spécifiques, inhérents au déroulement électronique de la consultation. Ainsi, il faut que les observateurs aient la possibilité, notamment, d'accéder aux informations pertinentes relatives au logiciel ; il faut qu'ils puissent voir les mesures de sécurité physiques et électroniques pour les serveurs ; qu'ils puissent inspecter et tester les dispositifs certifiés, avoir accès aux sites et aux informations concernant le vote électronique à distance et procéder aux tests appropriés ; enfin, observer le dépôt des bulletins électroniques, ainsi que le dépouillement. Toutefois, il peut s'avérer nécessaire, compte tenu des mesures de sécurité, de ne pas autoriser la présence d'observateurs dans la salle des ordinateurs. Dans ce cas, il conviendrait de prendre des mesures afin de donner aux observateurs la possibilité de contrôler les opérations.

Norme n° 35. « Des normes ouvertes seront utilisées… »

100. Permettre le recours aux systèmes ou services de vote électronique de différents fournisseurs implique une interopérabilité entre ces divers systèmes ou services. L'interopérabilité exige que les entrées et sorties soient conformes à des normes ouvertes et en particulier à des normes ouvertes en matière de vote électronique. Ces normes doivent être régulièrement mises à jour pour prendre en compte les développements juridiques et techniques.

101. Le fait de recourir à des normes ouvertes offre les principaux avantages suivants :

- elles offrent un choix plus vaste en termes de produits et de fournisseurs ;
- elles assurent une dépendance moindre vis-à-vis d'un seul fournisseur ;
- elles permettent d'éviter le blocage par des systèmes propriétaires ;
- elles offrent une stabilité ou une réduction des coûts ;
- elles s'accommodent plus facilement de modifications ultérieures.

102. Les pays, en particulier les pays décentralisés composés de différents États/membres et donc de diverses pratiques électorales, peuvent décider d'adopter ces normes au niveau national[4]. Au niveau régional, les pays peuvent décider d'adopter des normes régionales.

103. Au niveau international, le consortium international sur l'interopérabilité des activités électroniques OASIS a défini des normes pour les informations sur les services d'aide aux élections et aux électeurs fondées sur le langage XML. OASIS a conçu le langage de balisage pour les élections ou *Election Markup Language* (EML). Cet ensemble de données et de définitions de messages décrit comme un ensemble de schémas XML était la première norme internationale d'échanges structurés de données entre les moyens, matériels et logiciels, et les fournisseurs de services intervenant d'une manière ou d'une autre dans la fourniture de services d'aide aux élections ou aux électeurs. Sa fonction est la définition d'interfaces ouvertes, sûres, normalisées et interopérables entre les différents éléments des systèmes électoraux. Des informations complémentaires sur les travaux d'OASIS dans le domaine électoral (qui se sont achevés au milieu de l'année 2015) sont disponibles à l'adresse http://www.oasis-open.org/committees/election.

RESPONSABILITÉ

Norme n° 36. « Les États membres élaboreront des exigences… »

104. Les administrations électorales ou l'entité qu'elles auront désignée devraient élaborer des exigences techniques relatives aux systèmes de vote électronique. Elles devraient élaborer également des exigences pour les techniques d'évaluation allant des simples tests à une certification formelle des systèmes de vote électronique. Les profils de protection des Critères communs et les Critères communs (CC)/ISO 15408 contiennent des exigences de ce type.

105. Ces deux types d'exigences visent à assurer, avant d'utiliser effectivement le système de vote électronique au cours d'une élection ou d'un référendum, que le système est conçu conformément aux principes des élections démocratiques et fonctionne correctement, c'est-à-dire exactement comme prévu.

106. Il appartient à l'administration électorale ou à l'entité désignée par elle de veiller à ce que l'ensemble des exigences mentionnées soient totalement conformes aux principes juridiques pertinents des élections démocratiques. Ces exigences devront être mises à jour aussi souvent que nécessaire afin d'intégrer les évolutions juridiques éventuelles. Par exemple, les règles organisationnelles d'un type d'élection peuvent changer au fil du temps : tout comme les exigences respectives qui traduisent ces règles en instructions techniques relatives au système ou à sa certification.

Norme n° 37. « Avant la mise en service de tout système de vote électronique… »

107. Un contrôlé approprié d'un système de vote électronique permettra d'attester de la compatibilité du système avec les exigences techniques qui, ainsi qu'indiqué dans la disposition précédente, sont fondées sur les principes des élections démocratiques et ont pour objectif de les appliquer. La valeur ajoutée d'un tel contrôle n'est pas seulement d'établir si tel ou tel système de vote électronique est conforme aux exigences et normes définies ; il s'agit également d'un instrument important pour susciter la confiance dans ce système.

108. L'administration électorale doit veiller à la conformité du système de vote électronique avec les exigences techniques. Pour ce faire, elle devrait charger un organe indépendant et compétent d'évaluer le système. La notion d'indépendance de l'organisme implique une indépendance à la fois vis-à-vis du fabricant ou du fournisseur du système et du point de vue des ingérences politiques.

109. L'organisme indépendant peut être un organisme gouvernemental, tel qu'un office chargé de la certification de la sécurité informatique nationale, ou une organisation privée (nationale ou internationale), comme les laboratoires d'évaluation ou les agences de certification (comme celles qui sont accréditées pour assurer les programmes nationaux ou internationaux d'évaluation tels que le BS7799/Iso17799, les Critères communs ou Itsec). Quel que soit le cas, cet organisme devrait être habilité à effectuer un processus de certification, outre le fait d'être indépendant vis-à-vis du fabricant ou du fournisseur du système et du point de vue des ingérences politiques. Par ailleurs, sa nomination (en tant qu'organisme de certification) devrait se faire dans la transparence.

110. La certification ou un autre contrôle approprié doit se faire avant la mise en service de tout système de vote électronique, et à intervalles réguliers, chaque fois que nécessaire, c'est-à-dire après tout changement important apporté au système. Le processus de certification peut prendre différentes formes.

[4] C'est notamment le cas en Suisse, où les normes ont été mises en place par eCH, l'association de normalisation en matière de gouvernement électronique. Des informations complémentaires sur les normes relatives au vote électronique sont consultables sur ww.ech.ch sous *eCH Documents > nach Temenbereich > Politische Activitäten*.

Les États membres peuvent, par exemple, choisir de certifier le système de manière globale ou seulement certains de ses composants, gardant à l'esprit l'objectif de veiller à ce que le système et les procédures puissent répondre à d'éventuels menaces ou risques particuliers et respectent les normes des élections et référendums démocratiques.

Norme n° 38. « Le certificat, ou tout autre document approprié… »

111. Tout document approprié délivré devrait indiquer en toute transparence l'ensemble du processus d'évaluation et ses résultats ; les éléments ainsi certifiés devraient être réutilisables par toute partie tierce en particulier celles ayant accès au système. C'est sur la base de ce certificat que l'on pourra vérifier que tel ou tel système électoral est effectivement conforme aux éléments certifiés. Ainsi, le certificat devrait indiquer (au minimum) les données suivantes (ou indiquer de quelle manière s'y référer) :

- la personne ou le groupe ayant délivré le certificat ;
- la durée/les dates/les conditions de validation (par exemple, un accord de confidentialité) ;
- un exposé des objectifs du certificat ; et des indications concernant l'accessibilité du système, sa sécurité, son applicabilité, son bon fonctionnement, et le degré de ces divers éléments ;
- un exposé de la méthode de certification. Quelles normes ont été utilisées ? Quels sont les modes de contrôle et d'évaluation du système ? Quel est le mode d'analyse du code source ? Quel est le mode de vérification des composants matériels ? ;
- une description du système certifié. Pour en permettre la reproductibilité par des tierces parties, cette description doit intégrer des empreintes digitales numériques liées aux composants du logiciel, des spécifications précises des versions logicielles intégrées, ou encore les composants matériels – entre autres éléments ;
- les résultats du processus de certification ;
- des observations concernant les exigences opérationnelles et autres conditions préalables ;
- une empreinte digitale numérique liée au certificat ou système similaire.

Norme n° 39. « Le système de vote électronique pourra faire l'objet d'un audit… »

112. La vérification de la procédure, des ressources ou de l'infrastructure du système de vote électronique est le moyen susceptible d'établir une confiance et une assurance dans le fonctionnement des systèmes informatiques mis en œuvre pour le vote électronique. Cela implique l'intégrité et l'authenticité des informations d'audit et des systèmes d'audit mis en place.

113. Les audits visent à détecter les attaques éventuelles contre les systèmes. Une surveillance indépendante et extensive de la sécurité, la vérification, les contrôles croisés et les rapports sont des éléments vitaux des environnements de vote électronique. Un système d'élection électronique devrait donc prévoir des dispositifs d'audit pour chacun de ses principaux éléments (le vote, le dépouillement, etc.) et à différents niveaux du système : logique, des applications, technique.

114. Les dispositifs de vérification au niveau logique devraient principalement rendre compte de l'utilisation qui est faite du système. Les dispositifs de vérification au niveau des applications devraient fournir des informations sur les activités assurées par le système afin de permettre une reconstitution de son fonctionnement. Les dispositifs de vérification au niveau technique devraient fournir des indications sur les activités administrées par l'infrastructure utilisée. Il peut s'agir, par exemple, d'informations de routine sur des charges spécifiques, mais aussi d'informations spécifiques sur les signaux envoyés par un Système de détection d'intrusion (SDI) face à d'éventuelles attaques.

115. Les voies suivies par l'information d'audit sont déterminantes dans les systèmes de vote électronique ; elles doivent donc être aussi complètes que possible et ouvertes aux tiers qui voudraient les examiner. Il conviendrait que des données traitées par l'audit soient disponibles à divers points et niveaux des systèmes de vote électronique ; des données peuvent ainsi être vérifiées aux niveaux de l'EML, du système informatique ou des infrastructures de communication.

116. Le niveau de l'EML présente de nombreux points normalisés d'interface ouverte. Les flux de données peuvent être facilement observés et surveillés à ces points d'interface. Les systèmes de vérification devraient aussi viser les interfaces autres que celles de l'EML, comme celles de l'infrastructure de communication, des bases de données et des fonctions de gestion du système.

117. Des règles de procédure devraient également être élaborées afin de préciser l'utilisation des systèmes de vérification pendant le déroulement des élections ou des référendums, et des procédures prédéfinies devraient être mises en place pour assurer une réaction rapide.

118. Le système de vérification devrait permettre aux observateurs de suivre l'évolution du scrutin en temps réel sans révéler le décompte ou résultat final potentiel. Les observateurs devraient, par exemple, pouvoir suivre en temps réel le total des bulletins de vote déposés afin de pouvoir procéder à des contrôles croisés indépendants.

119. Le système d'audit ou de vérification devrait pouvoir déceler les fraudes des électeurs et fournir la preuve que tous les suffrages comptabilisés sont authentiques. Tout cas de tentative de fraude par des électeurs devrait être répertorié ; les listes de contrôle du système de vérification devraient comporter des données offrant la possibilité de réaliser des contrôles croisés du droit de vote et de vérifier que tous les suffrages comptabilisés ont été exprimés par des électeurs habilités à le faire, et que toutes les voix légitimes ont été comptabilisées.

120. Le système de vérification devrait collecter toutes les données dont les responsables électoraux ont besoin pour établir les correspondances et vérifier la présence de tous les suffrages exprimés, et ainsi s'assurer du fonctionnement correct du système de vote et de la légitimité du résultat. Il faut un décompte des bulletins de vote pour le comparer au total des suffrages exprimés, invalidés et nuls. Le système de vérification devrait fournir une possibilité indépendante de contrôle croisé et de vérification du bon fonctionnement du système électronique de vote ainsi que de l'exactitude du résultat. Le système de vérification devrait être capable d'établir qu'aucun suffrage authentique n'a été perdu et que tous les suffrages sont comptabilisés.

121. Les contrôles croisés des informations indépendantes de vérification augmentent les chances de déceler les attaques cachées contre les systèmes de vote électronique, ces attaques ne pouvant échapper aux contrôles que si elles sont cachées de la même manière dans le système de vote électronique et dans les informations indépendantes d'audit.

122. Le système d'audit devrait répondre aux mêmes exigences de sécurité que celles spécifiées pour la mise en œuvre du système de vote électronique proprement dit.

123. Le système d'audit doit lui-même être protégé contre les attaques visant à corrompre, à altérer ou à détruire des entrées. La détection de toute attaque intérieure ou extérieure contre le système d'audit doit être immédiatement signalée et suivie des mesures qui s'imposent.

FIABILITÉ ET SÉCURITÉ DU SYSTÈME

Norme n° 40. « L'administration électorale sera responsable… »

124. Outre le fait d'être disponible et utilisable, le mode de suffrage électronique doit être fiable et sûr afin de se conformer aux principes des élections démocratiques. Il appartient à l'État membre de s'en porter garant. La responsabilité générale incombe à l'administration électorale qui supervise le vote électronique et ne peut être déléguée, par exemple, à un fournisseur de systèmes de vote.

125. Le respect des principes doit être garanti aussi en cas de pannes ou d'attaques. Cela implique que le système de vote électronique doit être sûr, autrement dit solide pour résister aux attaques délibérées, et fiable, si par lui-même, il fonctionne, quelles que soient les déficiences du matériel ou du logiciel.

126. Les solutions techniques qui correspondent à l'état actuel de la technique sont revues par les pairs et largement approuvées par la communauté scientifique concernée contribuent à garantir la disponibilité, la fiabilité, la capacité effective d'utilisation et la sécurité du système de vote électronique même en cas de pannes ou d'attaques.

Norme n° 41. « Seules les personnes autorisées par l'administration électorale… »

127. Chaque intervention sur un équipement ou sur un logiciel présente en soi des risques techniques et humains. Il conviendrait donc de les minimiser pendant la durée d'une opération. C'est pourquoi il faut privilégier les contrôles automatiques et limiter les interventions à distance hors du contrôle des autorités. Si toutefois une intervention est rendue indispensable par les événements, il faudrait minimiser les risques d'intrusion, d'erreur humaine, de sabotage, etc., en définissant un protocole d'intervention qui devrait être suivi et validé, en limitant le nombre des personnes habilitées à intervenir à un petit groupe sous contrôle et en imposant également le contrôle de chaque intervention par la présence d'au moins deux personnes qualifiées et répondant aux règles de sécurité définies par l'autorité compétente.

Norme n° 42. « Avant toute élection électronique, l'administration électorale… »

128. Avant toute élection électronique, l'administration électorale vérifiera et établira elle-même que le système de vote électronique utilisé est bien celui qui doit être utilisé, autrement dit que le logiciel est authentique (le même que celui qui a été précédemment vérifié et autorisé) et fonctionne correctement.

129. Cette disposition devrait empêcher l'installation de systèmes de vote électronique ayant éventuellement fait l'objet de manipulations ou de remplacements touchant l'ensemble du système ou certains de ses éléments. L'administration électorale doit veiller à ce que les systèmes prévus soient utilisés. De plus, cette norme exige que le système fonctionne correctement.

Norme n° 43. « Une procédure sera établie… »

130. L'évolution permanente des nouvelles technologies de l'information et de la communication impose des mises à jour régulières (particulièrement) en ce qui concerne les logiciels. Cela nécessite des mises à jour tant de l'infrastructure centrale que des équipements de vote utilisés dans un environnement contrôlé (machine à voter). Toute mise à jour importante devra faire l'objet d'une certification similaire à la certification initiale avant de pouvoir être mise en exploitation.

131. Or, un système de vote électronique se doit de rester aussi transparent que possible tant pour les autorités que pour les citoyens. C'est pourquoi il faudrait publier une description précise, à jour et complète des éléments d'infrastructure, ce qui permettra aux personnes intéressées de s'assurer de la conformité des systèmes utilisés avec ce qui a été certifié par les autorités compétentes. Dans le même ordre d'idées, les résultats de la certification devraient être rendus disponibles aux autorités, aux partis politiques, voire, selon les règles en vigueur, aux citoyens.

Norme n° 44. « Les suffrages seront cryptés en cas de stockage ou de transmission… »

132. Dès que le suffrage a été enregistré, personne ne devrait plus être en mesure de le modifier ou de le relier à l'électeur qui l'a émis. C'est le but, entre autres mesures, de l'opération consistant à sceller l'urne et, dans le contexte du vote à distance, à sceller le suffrage durant son transfert entre l'électeur et l'urne au moyen d'un cryptage. Le suffrage est scellé lorsque son contenu a été soumis à des mesures faisant en sorte qu'il ne puisse être ni lu, ni modifié, ni relié à l'électeur qui l'a émis.

133. Sceller et protéger une urne électronique peut nécessiter des mesures physiques et techniques, telles que des contrôles d'accès, des structures d'autorisation et des murs pare-feu.

Norme n° 45. « Les votes et les informations relatives aux électeurs resteront scellés… »

134. Cette norme précise le moment où l'on déverrouille l'urne : juste avant le dépouillement. Comme indiqué ailleurs (et par analogie avec l'urne physique), avant cela, les votes sont mélangés.

Norme n° 46. « L'administration électorale manipulera… »

135. Cette norme rappelle que les procédures adéquates les plus modernes doivent être prévues pour manipuler le matériel crypté.

Norme n° 47. « En cas d'incident susceptible d'affecter l'intégrité du système… »

136. Il est important que les incidents qui affectent l'intégrité du système soient immédiatement rapportés à l'entité compétente responsable de la communication qui veille à ce que toutes les mesures requises soient prises et à ce que toutes les parties concernées, à savoir les partis politiques et les citoyens, soient dûment informées.

Norme n° 48. « L'authenticité, la disponibilité et l'intégrité des listes électorales… »

137. L'authentification de l'origine des données peut, par exemple, être assurée par des signatures électroniques dans les processus entièrement informatisés. Quand l'informatisation n'est que partielle, l'authentification de l'origine des données peut aussi s'appuyer sur des mesures de sécurité conventionnelles telles que les signatures manuelles, les cachets, les courriers, etc.

138. La liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme confère ce droit de vote. Il est à noter que les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter les suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire, cas de figure dans lequel il est essentiel de disposer d'une liste de ceux qui ont voté.

Norme n° 49. « Le système de vote électronique identifiera les suffrages… »

139. Il convient d'identifier les irrégularités afin de prendre les mesures qui s'imposent et afin que les parties concernées (électeurs, administration électorale, etc.) puissent être informées et soient en mesure de réagir en conséquence.