COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DÉLÉGUÉS DES MINISTRES Documents CM CM(2017)50-add2final 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)

b. Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique

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

Préambule

Le Comité des Ministres, en vertu de l'article 15.*b* du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une plus grande unité entre ses membres afin de préserver et de promouvoir ses idéaux et principes, qui sont leur patrimoine commun ;

Réaffirmant sa conviction que la démocratie représentative et directe fait partie de ce patrimoine commun et qu'elle sert de fondement à la participation des citoyens à la vie politique à l'échelle de l'Union européenne et aux niveaux national, régional et local ;

Vu les obligations et engagements acceptés dans le cadre des instruments et documents internationaux existants, tels que :

- la Déclaration universelle des droits de l'homme ;
- le Pacte international relatif aux droits civils et politiques ;
- la Convention des Nations Unies sur l'élimination de toutes les formes de discrimination raciale ;
- la Convention des Nations Unies sur l'élimination de toutes les formes de discrimination à l'égard des femmes ;
- la Convention des Nations Unies relative aux droits des personnes handicapées ;
- la Convention des Nations Unies contre la corruption ;
- la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (STE n° 5), et en particulier son Protocole additionnel (STE n° 9) ;
- la Charte européenne de l'autonomie locale (STE n° 122) ;
- la Convention sur la cybercriminalité (STE n° 185) ;
- la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) ;
- le Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181) ;
- la Convention sur les normes en matière d'élections démocratiques et les droits et libertés électoraux dans les États membres de la Communauté des États indépendants (CDL-EL(2006)031rev) ;
- la Recommandation n° R (99) 5 du Comité des Ministres aux États membres sur la protection de la vie privée sur internet ;
- la Recommandation Rec(2004)15 du Comité des Ministres aux États membres sur la gouvernance électronique (« e-gouvernance ») ;
- la Recommandation CM/Rec(2009)1 du Comité des Ministres aux États membres sur la démocratie électronique ;
- le document de la réunion de Copenhague de la Conférence sur la dimension humaine de l'OSCE ;
- la Charte des droits fondamentaux de l'Union européenne ;

- le Code de bonne conduite en matière électorale, adopté par le Conseil des élections démocratiques du Conseil de l'Europe et la Commission européenne pour la démocratie par le droit (Commission de Venise) et soutenu par le Comité des Ministres, l'Assemblée parlementaire et le Congrès des pouvoirs locaux et régionaux du Conseil de l'Europe ;

Ayant à l'esprit que le droit de vote est l'un des principaux fondements de la démocratie et que tous les modes de suffrage, y compris le vote électronique, doivent par conséquent être conformes aux principes des élections et des référendums démocratiques ;

Reconnaissant que l'utilisation des technologies de l'information et de la communication par les États membres dans le cadre des élections a considérablement progressé au cours des dernières années ;

Notant que certains États membres utilisent déjà ou se proposent d'utiliser le vote électronique à plusieurs fins, et notamment pour :

- permettre aux électeurs d'enregistrer leur suffrage à partir d'un lieu autre que le bureau de vote de leur circonscription électorale ;
- faciliter l'enregistrement de son suffrage par l'électeur ;
- faciliter la participation aux élections et aux référendums des citoyens autorisés à voter et résidant ou séjournant à l'étranger ;
- étendre l'accès au scrutin des électeurs souffrant d'un handicap ou se heurtant à d'autres difficultés pour se rendre en personne dans un bureau de vote et utiliser les installations qui s'y trouvent ;
- accroître la participation aux scrutins en proposant de nouveaux modes d'expression des suffrages ;
- adapter les élections à l'évolution de la société et à l'utilisation croissante des nouvelles technologies en tant que moyen de communication et de participation à la vie civique afin de faire progresser la démocratie ;
- réduire progressivement le coût global de l'organisation d'une élection ou d'un référendum pour les autorités électorales ;
- fournir plus rapidement et d'une manière fiable les résultats des scrutins ; et
- offrir aux électeurs un meilleur service en leur proposant plusieurs modes de suffrage ;

Reconnaissant l'intérêt de l'expérience acquise par les États membres qui ont eu recours au vote électronique ces dernières années et des enseignements tirés de cette expérience ;

Conscient également de l'expérience découlant de l'application de la Recommandation Rec(2004)11 du Comité des Ministres aux États membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique ; des Lignes directrices pour la conception de processus de confirmation du respect des exigences et normes recommandées (Certification des systèmes de vote électronique) et des Lignes directrices relatives à la transparence des élections par voie électronique ;

Réaffirmant sa conviction que la confiance du public dans les autorités chargées de la gestion d'élections est une condition préalable indispensable à l'introduction du vote électronique ;

Conscient des inquiétudes au sujet des problèmes de sécurité, de fiabilité ou de transparence que pourraient poser les systèmes de vote électronique ;

Conscient, par conséquent, que seuls des systèmes de vote électronique sûrs, fiables, efficaces, techniquement solides, ouverts à une vérification indépendante et aisément accessibles aux électeurs obtiendront du public la confiance nécessaire à l'organisation d'élections électroniques ;

Conscient de la nécessité pour les États membres de prendre en compte l'environnement dans lequel le vote électronique est mis en œuvre ;

Conscient que, compte tenu des récents développements techniques et juridiques relatifs aux élections par voie électronique dans les États membres du Conseil de l'Europe, les dispositions de ladite recommandation doivent être revues en profondeur et actualisées ;

Vu les travaux du Comité ad hoc d'experts sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (CAHVE), chargé par le Comité des Ministres de mettre à jour la Recommandation Rec(2004)11 ;

Adopte les lignes directrices suivantes sur les normes relatives au vote électronique, qui serviront d'outil pratique aux gouvernements des États membres pour l'approbation, l'adoption, la mise en œuvre et le suivi de l'approche qui y est décrite, ainsi que pour l'adaptation de leurs systèmes de vote électronique ;

Invite les gouvernements des États membres à s'assurer que les lignes directrices sont largement diffusées auprès des administrations électorales, du personnel chargé des élections, des citoyens, des partis politiques, des observateurs nationaux et internationaux, des organisations non gouvernementales (ONG), des médias, des universitaires, des fournisseurs de dispositifs de vote électronique et des organes spécifiques de contrôle du vote électronique.

Introduction

1. Les présentes lignes directrices sont la version révisée des Lignes directrices pour la conception de processus de confirmation du respect des exigences et normes recommandées (Certification des systèmes de vote électronique) et des Lignes directrices relatives à la transparence des élections par voie électronique. Ces deux documents originaux ont été approuvés en 2011 dans le but de donner des orientations sur la mise en œuvre des dispositions relatives à la certification et à la transparence contenues dans la Recommandation Rec(2004)11 du Comité des Ministres aux États membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique du 30 septembre 2004.

2. La Recommandation Rec(2004)11 et les lignes directrices originales ont été réexaminées et actualisées en 2015 et en 2016 par le Comité ad hoc d'experts sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (CAHVE) mis en place par le Comité des Ministres le 1er avril 2015.

3. Chaque ligne directrice sur la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 est identifiée par un numéro qui renvoie à la disposition correspondante de la recommandation.

4. La présente version des lignes directrices devra être complétée pour tenir compte de toutes les formes de vote électronique couvertes par la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique. Par ailleurs, compte tenu des évolutions permanentes dans les domaines juridique et technique, leurs dispositions devront être régulièrement mises à jour.

5. Les présentes lignes directrices sont destinées à être utilisées lors d'élections et de référendums politiques, à tous les niveaux de gouvernance. Elles n'entendent pas imposer aux États membres une ligne de conduite particulière quant à la mise en œuvre des dispositions de la recommandation révisée, mais visent plutôt à leur fournir des orientations et une aide en la matière.

6. Les présentes lignes directrices, tout comme la recommandation révisée, ne sauraient constituer un cadre réglementaire exhaustif concernant le vote électronique. Les États membres devront étendre leurs dispositions pour tenir compte des spécificités nationales dans le domaine électoral. Les lignes directrices incluent également des exemples de mise en œuvre des normes dans des contextes spécifiques, qualifiés de « bonnes pratiques ». Ces exemples sont donnés à titre d'information.

I. Lignes directrices pour la mise en œuvre des recommandations relatives au suffrage universel

1. Interface utilisateur du système de vote électronique sera facile à comprendre et à utiliser par tous les électeurs.

a. La présentation des options de vote sur le dispositif utilisé par l'électeur devrait être optimisée pour l'électeur moyen sans connaissances spécialisées en informatique.

Les dispositifs et services doivent pouvoir être adaptés aux restrictions fonctionnelles et à la situation particulière de l'utilisateur sans porter atteinte aux principes applicables tels que l'égalité. Cela peut se faire en proposant plusieurs versions différentes d'un même produit, des possibilités de modification des paramètres clés, une conception modulaire, des appareils auxiliaires ou d'autres moyens.

b. Il conviendrait d'associer les électeurs à la conception des systèmes de vote électronique, en particulier pour mettre en évidence d'éventuelles difficultés et tester leur facilité d'utilisation à chaque grande étape de leur élaboration.

L'accessibilité suppose que les systèmes soient conçus de manière à pouvoir être utilisés par le plus grand nombre d'électeurs possible. Les dispositifs et services doivent être fonctionnels et tenir compte des besoins du public, sans être inutilement complexes. Une bonne collaboration entre l'équipe de développement et un panel d'utilisateurs représentatif permettra de remplir ces exigences.

c. On devrait veiller, dès la conception, à assurer la compatibilité des nouveaux dispositifs avec ceux existants.

2. Le système de vote électronique sera, dans la mesure du possible, conçu de manière à permettre aux personnes handicapées et aux personnes ayant des besoins spéciaux de voter de façon autonome.

a. Les électeurs devraient se voir offrir, si la demande en est faite et que la possibilité existe, des services complémentaires tels que des interfaces spéciales ou d'autres ressources équivalentes, comme une assistance personnelle.

Le vote électronique peut constituer un moyen d'élargir les possibilités de vote autonome offertes aux personnes handicapées et aux personnes ayant des besoins spécifiques. Un juste équilibre devrait être trouvé entre la mise à disposition de ces nouvelles possibilités d'accès au vote et le respect d'autres exigences, en l'occurrence celles de la sécurité du vote électronique.

b. Les interfaces de vote par internet devraient, autant que possible, être conformes aux directives de l'Initiative d'accès au web (Web Accessibility Initiative-WAI).

En vue d'assurer un haut niveau d'accessibilité du web aux personnes handicapées, le W3C (Consortium du World Wide Web créé en 1994 pour optimiser le potentiel du web mondial au moyen de protocoles communs) a lancé la WAI qui vise à rendre le web accessible en menant des actions dans cinq grands domaines : les technologies du web, l'élaboration de lignes directrices, la conception d'outils, l'éducation et la formation ainsi que la recherche et le développement. La WAI a déjà produit un ensemble de normes et de lignes directrices en faveur de l'accessibilité (parmi lesquelles les Règles pour l'accessibilité des contenus web et Directives pour l'accessibilité aux contenus web, les Règles d'accessibilité pour les outils d'édition, les Directives pour l'accessibilité des agents utilisateurs, les XML Accessibility guidelines, etc.). Pour de plus amples informations, consulter le site internet de la WAI à l'adresse : www.w3.org/WAI.

La WAI est généralement utilisée dans le cadre des solutions de vote par internet reposant sur des logiciels de navigation. Ses principes généraux peuvent toutefois être appliqués même lorsque d'autres solutions de vote par internet sont mises en œuvre (par exemple lorsque l'application de vote est elle-même un navigateur distinct).

II. Lignes directrices pour la mise en œuvre des recommandations relatives au suffrage légal

5. Toutes les informations officielles relatives au scrutin seront présentées de manière équivalente dans l'ensemble des modes de suffrage.

a. Le bulletin électronique servant à enregistrer le suffrage devrait être exempt de toute information sur les options de vote, autre que celle requise par la loi.

L'interface de vote électronique ne devrait pas contenir davantage d'informations relatives aux options en présence que les bulletins officiels (généralement papier). Elle ne devrait pas non plus contenir d'éléments tels que des fenêtres pop-up visant à promouvoir un candidat ou un point de vue, ni d'éléments audio associés à un candidat ou à un point de vue particulier. Aucune information non mentionnée sur le bulletin papier ne devrait y figurer (égalité des modes de suffrage). Cela n'interdit pas l'affichage d'informations officielles sur les options de vote.

b. Si des informations sur les options de vote sont accessibles à partir du site de vote électronique, ces informations seront présentées de manière égale.

Les informations relatives aux options de vote devraient être présentées de manière égale dans l'ensemble des modes de suffrage.

9. Le système de vote électronique fera en sorte que seul le nombre approprié de suffrages par électeur soit enregistré et stocké dans l'urne électronique, et inclus dans le résultat de l'élection.

a. Si un électeur a la possibilité d'exprimer un suffrage plusieurs fois par voie électronique, des mesures appropriées devraient être prises pour faire en sorte de ne comptabiliser qu'un seul vote.

b. Si un électeur a la possibilité d'exprimer un suffrage par le biais de plusieurs modes de suffrage, des mesures appropriées devraient être prises pour faire en sorte de ne comptabiliser qu'un seul vote.

Lignes directrices 9a et 9b : Lorsque les votes multiples sont autorisés, ils devraient également l'être dans le cadre des élections électroniques. Certains systèmes de vote permettent par exemple aux électeurs de voter à l'avance une ou plusieurs fois et de changer d'avis ultérieurement. Seul le dernier vote est alors déposé dans l'urne et prend valeur de suffrage. C'est le cas à Andorre, au Danemark et en Suède.

L'option du vote multiple (expression d'un suffrage plusieurs fois par voie électronique ou par le biais de plusieurs modes de suffrage) peut être introduite dans le cadre du vote électronique pour faire face au risque de pressions sur les électeurs, qui reste présent lorsque le vote a lieu en dehors d'un environnement contrôlé (vote à distance). Cette possibilité existe en Estonie.

On définira au niveau national quel vote doit être pris en considération. Dans le contexte du vote électronique, un pays pourra décider que le vote papier a la priorité. Ailleurs, seul le dernier suffrage exprimé sera comptabilisé. Un autre pays pourra décider que le premier suffrage valablement exprimé est celui qui compte. Pour être conforme aux principes des élections démocratiques, le système de vote électronique (ou le recours simultané au vote par bulletin papier et au vote électronique) doit assurer un suffrage égal. Dans le cas du vote multiple, la question de savoir quel suffrage doit être pris en compte sera traitée dans la législation nationale. Le principe « une personne, une voix » doit être respecté.

La décision de savoir quel vote est pris en compte dépendra de la politique nationale en vigueur concernant le vote à distance. Les pays qui appliquent une politique plus stricte en la matière donneront généralement la priorité au vote papier si c'est ce mode de suffrage qui est utilisé dans les bureaux de vote (environnement contrôlé). Les pays plus ouverts au vote à distance pourront décider que le vote qui compte est le premier suffrage valablement exprimé, auquel cas le vote électronique soumis à partir d'un environnement non contrôlé pourrait l'emporter sur un vote papier exprimé par la suite. Il appartiendra au législateur national de prendre les décisions qui s'imposent sur la manière de faire face au problème des pressions exercées sur les électeurs dans le contexte du vote à distance (de manière générale). Ces décisions ne devraient pas être laissées à la seule appréciation de l'administration responsable du vote électronique, car elles concernent la politique relative au vote à distance en général et non uniquement la mise en œuvre du vote électronique.

c. Dans tous les autres cas, des mesures appropriées devraient être prises pour empêcher tout électeur de voter plusieurs fois.

Dans les pays où le vote multiple n'est pas autorisé, les votes multiples sont considérés comme une tentative d'enregistrer davantage de suffrages que ceux auxquels un électeur donné a droit. Ce risque peut apparaître, par exemple, lorsqu'un électeur tente d'enregistrer lui-même des suffrages multiples ou quand une autre personne essaie d'usurper l'identité d'un électeur pour voter en son nom après que celui-ci a voté.

Dans le contexte du vote papier, des mesures organisationnelles permettent de maîtriser ce risque. Par exemple, au Royaume-Uni, si une personne constate à son arrivée au bureau de vote que quelqu'un d'autre a déjà voté en son nom, elle peut voter avec un bulletin spécial. Celui-ci n'est pas déposé dans l'urne, mais scellé dans une enveloppe ; il ne sera dépouillé qu'à la demande d'un tribunal saisi d'une requête en contestation du scrutin. Une disposition analogue s'applique lorsque deux votes sont reçus par correspondance pour un seul et même électeur. Des mesures appropriées doivent être envisagées dans le contexte du vote électronique. Il importe que l'identification soit sécurisée. Une solution pourrait être de conserver pendant une certaine durée le lien entre les codes d'identification de l'électeur et son bulletin scellé.

L'introduction du vote électronique à distance soulève la question de la corrélation entre les plages de temps pour le dépôt des bulletins dans les bureaux de vote et celles pour le vote électronique à distance. De prime abord, il semblerait logique que les périodes soient les mêmes dans les deux cas, afin d'éviter les complications et les distinctions. Il existe néanmoins plusieurs cas de figure dans lesquels la définition de périodes différentes semblerait plus appropriée :

- *d'une part, lorsque le dépôt d'un bulletin dans un bureau de vote est la solution de repli proposée aux électeurs qui se trouvent sur le territoire national de la consultation en cas de panne du système de vote électronique, la clôture du moyen de vote électronique doit intervenir avant celle du bureau de vote ;*

- *d'autre part, lorsque le système est conçu et mis en œuvre de telle manière que les électeurs peuvent choisir entre plusieurs modes de suffrage, mais que ces derniers ne sont pas rattachés à une liste commune permettant de voir quels électeurs ont déjà voté, il convient, d'une manière générale, d'éviter tout chevauchement entre les plages de temps pendant lesquelles ces modes de suffrage sont disponibles.*

En toute hypothèse, le décompte ne devrait commencer qu'après la clôture de tous les modes de suffrage.

d. Dans tous les cas, l'électeur devrait être clairement informé des possibilités de vote qui lui sont offertes et des règles applicables en matière de décompte des suffrages.

Il est particulièrement important d'informer l'électeur de la possibilité de voter plus d'une fois par voie électronique ou plusieurs fois successivement par le biais de modes de suffrage différents, lorsque le vote multiple est autorisé.

Dans tous les cas, l'électeur devrait être informé des règles applicables en matière de dépouillement ; il devrait notamment savoir quel sera le vote finalement pris en considération lors du décompte.

III. Lignes directrices pour la mise en œuvre des recommandations relatives au suffrage libre

10. L'intention de l'électeur ne sera pas affectée par le système de vote et sera à l'abri de toute influence indue.

a. En cas de vote électronique à distance, l'électeur devrait être informé des moyens de vérifier que la connexion est établie avec le serveur officiel et qu'un bulletin authentique lui est présenté.

Dans le contexte du vote électronique à distance, il faut envisager entre autres éventualités que de faux serveurs soient présentés, par exemple en imitant un serveur officiel par manipulation du système de noms de domaine (DNS), par l'utilisation d'un nom de domaine semblable à celui du serveur officiel, ou par corruption du code serveur (par exemple au moyen de logiciels malveillants). Les électeurs sont informés des moyens de vérifier le certificat du site officiel de vote électronique. L'apposition d'une signature électronique sur le bulletin par les autorités électorales permet de vérifier le bulletin. Ces mesures ne doivent cependant pas compromettre le caractère secret du vote.

b. Le système de vote électronique ne devrait pas autoriser que la volonté de l'électeur pendant le vote subisse d'influence et que celui-ci soit manipulé. En particulier, le bulletin électronique servant à enregistrer le suffrage devrait être exempt de toute information non authentique.

À l'instar de la disposition 5.a, cette ligne directrice vise à faire en sorte que l'électeur n'ait accès qu'à des informations officielles sur le vote et à ce qu'aucune influence ayant pour but d'affecter sa volonté ne puisse être exercée par des personnes sans autorisation.

c. Toutes les mesures envisageables devraient être prises dans le système de vote électronique pour éviter les influences destinées à manipuler le vote après son enregistrement, et des dispositions permettant de s'assurer qu'aucune influence de ce type n'a été exercée.

Le suffrage libre protège également le scrutin contre toute tentative de manipulation après l'enregistrement du suffrage. Il s'agit bien évidemment d'éviter toute influence manipulatrice ou intervention non autorisée sur le scrutin. Bien entendu, s'il est autorisé, le vote multiple n'est pas concerné par cette disposition et l'électeur devrait pouvoir voter plusieurs fois.

Cette disposition vise à empêcher toute modification non autorisée du vote une fois qu'il a été enregistré. Elle assure la protection du système contre les attaques venant de l'extérieur, mais aussi contre les menaces internes. La vérifiabilité individuelle et la vérifiabilité universelle (voir normes 15 et 17) permettent de détecter toute intervention non autorisée de ce type.

d. Lorsque cela est jugé nécessaire, le système de vote électronique devrait proposer des mécanismes (tel le vote multiple) pour protéger les électeurs contre toute manœuvre qui les contraindrait à voter d'une certaine manière.

Le vote multiple est considéré comme un moyen de protéger l'électeur contre d'éventuelles pressions, car il lui permet de revoter.

12. La manière dont les électeurs sont guidés durant la procédure de vote électronique ne les amènera pas à voter dans la précipitation ou sans confirmer leur choix.

a. Les électeurs devraient pouvoir modifier leur choix à n'importe quelle étape de la procédure de vote électronique à distance avant l'enregistrement de leur suffrage, ou interrompre la procédure.

Cette disposition prévoit la possibilité d'interrompre la procédure avant l'enregistrement du vote, c'est-à-dire avant qu'il soit déposé dans l'urne électronique. Une fois le vote enregistré, cette possibilité n'existe plus. L'interface doit donc être programmée de manière à attirer l'attention des électeurs sur ce point, par exemple en leur demandant de confirmer leur intention avant d'enregistrer le vote. Il est également utile de leur rappeler que cette opération validera le vote et le rendra définitif, si le vote multiple n'est pas autorisé.

15. L'électeur devra pouvoir vérifier que son intention est représentée avec exactitude dans le suffrage exprimé et que le vote scellé est parvenu à l'urne électronique sans avoir été modifié. Toute influence indue ayant modifié le suffrage pourra être détecté.

a. Lorsque le vote électronique est mis en œuvre dans les bureaux de vote, les États membres devraient envisager le recours à des bulletins papier comme deuxième support d'enregistrement des voix exprimées, à des fins de vérification.

Une méthode consiste à éditer des reçus papier à l'issue du vote – « voter-verified-paper-audit-trail », littéralement « traces papier vérifiables par l'électeur » –, elle vise à assurer le suffrage libre lorsque le vote s'effectue sur des machines à voter dans des environnements contrôlés. Si la solution électronique mise en œuvre dans les bureaux de vote est une forme de lecture optique du bulletin de vote, ce deuxième support ne sera pas nécessaire, car, par définition, le bulletin sera dans ce cas un bulletin papier.

Il existe d'autres solutions mettant en œuvre un deuxième support, par exemple des parties détachables sur le bulletin pour assurer la vérifiabilité individuelle (tel le modèle scantegrity de Chaum). Ces supports peuvent être très semblables aux reçus papier, mais se présenter sous une autre forme. Dans tous les cas, il s'agit de supports papier, à la fois inaltérables et lisibles/vérifiables à l'œil nu.

Les questions relatives à la validité de ce deuxième support seront traitées dans les réglementations nationales qui définiront également la marche à suivre en cas de divergences entre les résultats électroniques et ceux produits par le deuxième support en question.

b. Il conviendrait de procéder à un décompte obligatoire des voix à partir de ce deuxième support dans un nombre statistiquement significatif de bureaux de vote sélectionnés de façon aléatoire, notamment pour les machines à voter et les dispositifs de lecture optique des bulletins de vote.

Les critères tels que le pourcentage de votes concernés ou le nombre de bureaux de vote dans lesquels ce décompte aura lieu, leur désignation, etc. seront établis au niveau national. Ils devraient veiller à ce que le but général d'assurer des élections libres soit atteint.

IV. Lignes directrices pour la mise en œuvre des recommandations relatives au suffrage secret

19. Le vote électronique sera organisé de manière à garantir à toutes les étapes de la procédure que le secret du scrutin est respecté.

a. Les éléments relatifs à la liste électorale devraient être clairement séparés des éléments relatifs au vote proprement dit.

Cette disposition s'applique plus particulièrement aux techniques biométriques d'identification de l'électeur pouvant être utilisées dans les bureaux de vote en plus des machines à voter ou des dispositifs de lecture optique des bulletins de vote. La séparation des deux éléments permet d'assurer le secret du vote.

Lorsque les suffrages et les informations anonymisées sur les électeurs sont conservés ensemble, ils doivent être protégés par un cryptage du début à la fin.

21. Le système de vote électronique et toute partie autorisée protégeront les données d'authentification de manière à empêcher des parties non autorisées de détourner des données, de les intercepter, de les modifier ou d'en prendre connaissance de toute autre manière.

a. L'authentification devrait être fondée sur la cryptographie.

Cette disposition entend faire en sorte que les solutions techniques les plus avancées soient mises en œuvre pour protéger les données d'authentification.

23. Le système de vote électronique ne fournira pas de preuve du contenu du suffrage enregistré à l'électeur aux fins d'une utilisation par des tiers.

a. Quand une preuve papier du vote électronique est remise à l'électeur dans un environnement contrôlé, cet électeur ne devrait avoir aucune possibilité de la montrer à un tiers ou de l'emporter à l'extérieur du bureau de vote.

Le vote électronique ne devrait pas donner à l'électeur une preuve du contenu de son vote. Lorsque cette possibilité est prévue dans la procédure de vote, comme cela peut être le cas lors de l'utilisation de machines à voter dans les bureaux de vote, des mesures organisationnelles devraient être prises pour empêcher toute utilisation de cette preuve de nature à compromettre le secret du vote. Le but de ces mesures est de protéger le secret du vote et de se prémunir de la pratique de l'achat de voix. Il va de soi, dans l'absolu, que cela n'empêche pas l'électeur de divulguer le contenu de son bulletin, par exemple en le prenant en photo. De telles violations du secret du vote seront sanctionnées conformément aux dispositions du droit pénal ou administratif interne, qui s'appliquent également au vote électronique.

b. Aucune information résiduelle relative à la décision de l'électeur ne devrait être affichée après que le suffrage a été exprimé.

L'expression « informations résiduelles » désigne les informations qui restent accessibles en divers endroits (par exemple la mémoire de l´ordinateur personnel, le cache du navigateur, la mémoire vidéo, les fichiers d'échange (swap), les fichiers temporaires, etc.) après l'enregistrement du suffrage, et qui sont susceptibles de révéler la décision de l'électeur.

Cette disposition recommande aux concepteurs de systèmes ou aux prestataires de services de concevoir le système de vote électronique de manière à ce que les informations résiduelles soient effacées dès l'enregistrement du suffrage. Cela peut se révéler difficile sur le plan technique dans le cas du vote à distance. Quoi qu'il en soit, toutes les mesures envisageables devraient être prises pour assurer la suppression de ces informations résiduelles dès l'enregistrement du suffrage. La vérifiabilité individuelle pourra néanmoins être mise en œuvre s'il existe des garanties appropriées contre l'exercice de pressions sur l'électeur ou l'achat de voix.

c. En cas de vote électronique à distance, l'électeur devrait être informé des risques potentiels pour le secret du vote et se voir recommander des moyens de réduire ces risques avant le vote.

d. En cas de vote électronique à distance, l'électeur devrait être informé de la marche à suivre pour supprimer, si cette possibilité existe, toute trace de son vote sur l'appareil utilisé pour enregistrer celui-ci.

Lignes directrices 23c et 23d : Dans le cas du vote électronique à distance, les électeurs devraient être clairement informés du risque de violation du secret du vote, et des mesures et bonnes pratiques à adopter pour contrer ce risque, par exemple l'utilisation de pare-feu, la suppression des traces, etc. Le système lui-même devrait effacer automatiquement le plus de traces possible.

Le vote électronique à distance depuis un environnement non contrôlé implique un partage de responsabilités entre l'électeur et le système de vote électronique/l'administration électorale. Il est de la responsabilité de l'électeur d'adopter toutes les recommandations (figurant dans la présente disposition). Il appartient à l'autorité électorale de donner à l'électeur des informations claires sur trois points au moins : le principe du partage des responsabilités ; les différentes mesures à adopter par l'électeur pour réduire les risques (installation d'un logiciel antivirus, pare-feu, suppression des traces du vote, etc.) ; ainsi que les risques associés et les techniques permettant d'assurer la vérifiabilité.

Ces informations devraient parvenir à l'électeur bien avant la période électorale. C'est sur cette base que l'électeur pourra choisir d'utiliser ou non le vote électronique à distance.

Des messages d'avertissement pourraient s'afficher au début de la procédure de vote électronique et un message sur les mesures recommandées après le vote (suppression des traces, etc.) pourrait être transmis à l'électeur à la fin de la procédure. Ces messages ne constitueront toutefois que des rappels et ne remplaceront pas les informations initiales complètes que l'électeur devrait recevoir bien avant le début de la période du vote électronique.

26. La procédure de vote électronique, en particulier au moment du décompte des voix, sera organisée de sorte qu'il ne soit pas possible d'établir un lien entre le suffrage non scellé et l'électeur. Les suffrages sont, et restent, anonymes.

a. Les informations relatives à l'électeur devraient être séparées de la décision de l'électeur à une étape prédéfinie du processus de décompte.

b. Tout décodage nécessaire au dépouillement des voix devrait intervenir dès que possible après la clôture de la période du scrutin.

L'expression « informations relatives à l'électeur » désigne les données anonymisées sur l'électeur, telles que les codes d'identification utilisés dans le vote électronique à distance. Bien que le lien entre ces informations et le vote scellé doive être maintenu pendant une certaine durée sous une protection appropriée, pour ménager notamment la possibilité d'un vote multiple tout en respectant le principe « une personne, une voix », il devrait être détruit avant le dépouillement.

Le cryptage des bulletins est généralement nécessaire pour assurer l'anonymat du vote. Très souvent, le bulletin est crypté avant d'être transmis par les réseaux informatiques ; il est conservé crypté dans l'urne et il est décodé avant le dépouillement. Celui-ci est effectué avec des bulletins décodés, qui ne peuvent être mis en corrélation avec tel ou tel électeur.

Toutefois, il existe des méthodes de chiffrement qui ne nécessitent pas un décodage avant le dépouillement (chiffrement homomorphe). Le dépouillement peut ensuite intervenir sans que soit révélé le contenu des suffrages cryptés. Dans certains cas, il peut même être nécessaire, pour assurer l'anonymat, de procéder au dépouillement alors que les bulletins sont encore cryptés.

c. Les États membres devraient prendre les mesures nécessaires pour garantir la confidentialité de toute information obtenue par toute personne participant à un audit.

De plus, les mesures de protection des informations recueillies par le système d'audit contre les accès non autorisés devront s'accompagner de mesures juridiques et organisationnelles pour contrôler les personnes ayant un accès autorisé au système d'audit. Le processus d'accréditation pourrait, par exemple, comporter de telles mesures.

V. Lignes directrices pour la mise en œuvre des recommandations concernant la réglementation et l'organisation

27. Les États membres qui mettent en place le vote électronique le feront de manière graduelle et progressive.

a. Une étude de faisabilité formelle devrait être réalisée et publiée avant le choix et la mise en œuvre d'une technologie de vote électronique. Elle devrait indiquer les raisons de l'adoption de ce système et comporter une analyse des risques, une évaluation du cadre juridique, la planification des actions pilotes et leur évaluation ainsi qu'une analyse coûts-avantages.

b. La mise en œuvre de projets pilotes de vote électronique devrait débuter bien avant les élections et comprendre des préparatifs essentiels tels que l'adoption de règles détaillées, si cela se révèle nécessaire, pour les actions pilotes et le test du système.

c. La version finale du système de vote électronique devrait être testée avant que ce système soit utilisé dans le cadre d'élections ordinaires contraignantes.

d. Les projets pilotes devraient être menés sur la base de critères clairs et complets pour évaluer l'efficacité et l'intégrité du système de vote électronique, notamment en ce qui concerne la transmission des résultats.

28. Avant l'introduction du vote électronique, les États membres apporteront les modifications nécessaires à la législation pertinente.

a. Le cadre juridique devrait comporter des procédures pour la conduite du vote électronique, de la phase de mise en place jusqu'au dépouillement.

Les dispositions détaillées applicables en la matière se trouveront probablement dans des réglementations et instructions de niveau inférieur. Cela devrait être assuré par une législation de niveau supérieur qui devrait également clarifier les responsabilités pour l'adoption de telles dispositions détaillées.

b. Le cadre juridique devrait comporter des règles pour déterminer la validité d'un vote électronique.

c. Le cadre juridique devrait comporter des règles en cas de problèmes, de défaillances ou de divergences découlant de l'utilisation d'outils de contrôle.

Dans les États membres qui utilisent un deuxième support d'enregistrement des voix et procèdent systématiquement à un deuxième décompte des suffrages, des divergences de résultats entre les deux méthodes peuvent apparaître. Les règles devraient alors préciser quel type de vote (le vote électronique ou l'autre méthode) fait foi. L'un des arguments en faveur du vote électronique est que c'est la méthode par le biais de laquelle les électeurs se sont exprimés. Mais l'on pourrait également privilégier le deuxième support en faisant valoir que ce vote aurait pu être vérifié par les électeurs eux-mêmes, notamment lorsque le support en question inclut l'émission de reçus papier.

Par conséquent, en cas de divergence, il convient de procéder à un examen approfondi de la situation sur la base duquel seront prises toutes les décisions relatives au résultat du vote en question. Il est demandé aux États membres d'établir des règles concernant le mode de suffrage à prendre en compte pour le dépouillement officiel du scrutin, les conditions dans lesquelles un deuxième décompte des voix est jugé nécessaire, les modalités du décompte obligatoire, les circonstances dans lesquelles il est procédé au décompte de toutes les voix enregistrées sur le deuxième support, ainsi que celles dans lesquelles il convient d'organiser de nouvelles élections.

d. Le cadre juridique devrait contenir des procédures définissant les modalités de destruction de données, afin d'assurer notamment la conformité du traitement, du stockage et de la destruction des données (et du matériel) du vote électronique avec la législation relative à la protection des données à caractère personnel.

Le moyen de stockage qui contenait les votes (disque dur, clé USB, etc.) devrait être détruit.

e. Le cadre juridique devrait comporter des dispositions applicables aux observateurs nationaux et internationaux.

Les États membres devraient prévoir le rôle des observateurs nationaux et internationaux dans le processus de vote électronique et réglementer cet aspect, conformément à leurs engagements internationaux et aux bonnes pratiques en la matière. Le type « d'accès » au vote électronique accordé aux observateurs dépendra des dispositions nationales applicables. Celles-ci devraient être conformes aux engagements internationaux comme ceux du Bureau des institutions démocratiques et des droits de l'homme de l'Organisation pour la sécurité et la coopération en Europe (OSCE/BIDDH). Les observateurs devraient comprendre des représentants des partis politiques et du grand public.

f. La législation devrait établir un calendrier clair de toutes les étapes de l'élection électronique.

Par rapport aux modes de suffrage traditionnels, une élection électronique peut présenter des différences ayant trait par exemple à la période pendant laquelle les votes peuvent être émis, aux démarches à effectuer pour pouvoir participer à l'élection électronique et au déroulement concret du vote électronique. Ces différences devraient être clairement communiquées aux électeurs pour qu'ils disposent de tous les éléments nécessaires pour choisir leur mode de suffrage, mais aussi pour éviter toute méprise concernant les procédures applicables. Il convient de prendre en considération le temps nécessaire aux électeurs pour prendre cette décision.

g. La période pendant laquelle un vote électronique pourra être enregistré ne devrait pas commencer avant la notification du scrutin ou du référendum.

Il est particulièrement important de communiquer aux électeurs des informations sur la période durant laquelle un vote peut être émis lorsque celle qui s'applique au vote électronique est différente de celle qui s'applique aux autres modes de suffrage. Cette différence concerne plus particulièrement le vote électronique à distance où il peut être préférable d'instaurer une période de vote distincte, en raison de la nature spécifique de ce mode de suffrage.

h. Le vote électronique à distance pourra commencer et/ou se terminer avant les heures d'ouverture de tout bureau de vote.

i. La période pendant laquelle un vote électronique peut être enregistré ne devrait pas se poursuivre après la clôture du scrutin.

Lignes directrices 28h et 28i : Pour différentes raisons, la période d'ouverture du vote électronique à distance peut être plus longue que la période d'ouverture des bureaux de vote. Une telle mesure permet notamment d'offrir aux citoyens une accessibilité et une qualité de service accrues.

Le vote électronique à distance ne devrait pas, cependant, se poursuivre après la clôture du scrutin dans les bureaux de vote. En cas d'indisponibilité du système de vote électronique (par exemple si l'ordinateur d'un électeur est hors service à la suite d'une panne de courant), un électeur résidant ou séjournant sur le territoire national de la consultation (élection ou référendum) devrait encore pouvoir voter en bureau de vote. Si le vote électronique se poursuivait après la fermeture des bureaux de vote, les électeurs n'auraient pas cette possibilité.

j. Autoriser le dépôt des suffrages électroniques dans l'urne électronique devrait toutefois se poursuivre pendant un délai suffisant à l'issue de la période du scrutin électronique pour tenir compte des éventuels retards de transmission des messages par différents modes de vote électronique à distance.

k. À l'issue de la période du scrutin électronique, aucun électeur ne devrait plus avoir accès au système de vote électronique.

Lignes directrices 28j et 28k : Ces dispositions traitent des sessions de vote sur internet qui commencent peu avant la clôture du scrutin électronique. L'urne devra rester ouverte pour pouvoir recueillir ces derniers suffrages, pendant une durée équivalente à la durée normale d'une session de vote électronique, de manière à ce que les électeurs qui ont pu accéder au système quelques secondes avant sa fermeture puissent terminer normalement le processus de vote électronique.

Un autre cas de figure, également dans un scénario de vote par internet, serait celui où les services seraient momentanément surchargés juste avant la fin du scrutin, auquel cas l'enregistrement du vote dans l'urne électronique pourrait prendre davantage de temps. Les votes transmis dans les délais ne devraient pas être écartés en raison de tels retards. Le traitement des suffrages ne doit pas cesser immédiatement après la clôture du scrutin électronique. En revanche, il ne devrait pas être possible de commencer une session de vote électronique après la fermeture du service.

29. La législation pertinente réglementera les responsabilités concernant le fonctionnement des systèmes de vote électronique et fera en sorte que l'administration électorale en ait le contrôle.

a. Les processus de passation de marchés relatifs au vote électronique devraient être menés en toute transparence.

b. Des dispositions devraient être formulées pour éviter tout conflit d'intérêts d'acteurs privés intervenant dans le processus.

c. Une séparation stricte des fonctions sera assurée, preuves à l'appui.

d. Les États membres devraient prendre des mesures appropriées pour éviter que les élections reposent indûment sur les fournisseurs de services.

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

a. Un procès-verbal du dépouillement des votes électroniques devrait être établi, avec les heures de début et de fin de l'opération ainsi que des informations sur les personnes qui y ont participé.

b. Le dépouillement devrait être reproductible. Il devrait pouvoir être prouvé, par exemple au moyen d'un nouveau décompte indépendant, que la procédure de dépouillement a été menée de façon satisfaisante.

Le but de cette disposition est de faire en sorte que des preuves solides du bon déroulement de la procédure de dépouillement puissent être obtenues. Une possibilité serait de procéder à un nouveau décompte indépendant si celui-ci est effectué à l'aide d'un autre système issu d'une source différente, mais il existe encore d'autres solutions, telle la preuve cryptographique (vérifiabilité universelle).

c. D'autres caractéristiques du système de vote électronique susceptibles d'influer sur l'exactitude du résultat devraient être vérifiables.

Selon le système utilisé, des éléments autres qu'un nouveau décompte peuvent contribuer à garantir l'exactitude du résultat, par exemple la confirmation du fait que tous les suffrages exprimés ont bien été pris en compte.

Outre les outils de vérification, le pourcentage de votes exprimés par vote électronique et la comparaison des résultats du vote électronique par rapport aux résultats du vote par d'autres modes de suffrage doivent être pris en compte pour contrôler la vraisemblance des résultats du vote électronique et valider ainsi leur exactitude.

d. Le système de vote électronique devrait assurer, aussi longtemps que nécessaire, la disponibilité et l'intégrité des urnes électroniques et du résultat du dépouillement.

Les informations renfermées dans l'urne électronique doivent être préservées aussi longtemps que nécessaire pour permettre d'éventuels nouveaux décomptes, une contestation devant les tribunaux ou toute autre procédure prévue par la loi dans l'État membre concerné.

VI. Lignes directrices pour la mise en œuvre des recommandations relatives à la transparence et à l'observation

31. Les États membres feront preuve de transparence pour tous les aspects du vote électronique.

a. Les autorités électorales compétentes devraient publier une liste officielle des logiciels utilisés lors d'une élection électronique. Celle-ci contiendra au minimum les logiciels utilisés, leur version et leur date d'installation, ainsi qu'une brève description.

Les évolutions constantes des technologies de l'information et de la communication imposent des mises à jour fréquentes des matériels et logiciels, ainsi que l'adaptation régulière des systèmes centraux et des équipements de vote utilisés dans un environnement contrôlé (machines à voter, par exemple). Pour maintenir la transparence du vote électronique, des descriptions actualisées, complètes et exactes des matériels et logiciels devraient être publiées afin de permettre aux groupes intéressés de vérifier par eux-mêmes que les systèmes utilisés correspondent à ceux qui ont été certifiés par les autorités compétentes. Les résultats de la certification devraient être communiqués aux autorités, aux partis politiques et, si les dispositions juridiques en vigueur le prévoient, aux citoyens.

b. L'accès du public aux différents éléments du système de vote électronique et aux informations sur le sujet, en particulier les documents, le code source et les accords de confidentialité, devrait être communiqué bien avant le début de la période électorale.

Lorsque les résultats obtenus au moyen d'un appareil/système électronique ont force exécutoire, les éléments techniques qui déterminent les modalités de calcul peuvent devenir tout aussi importants qu'une loi électorale définissant les règles à appliquer par les bureaux de vote pour le dépouillement. Pour garantir la confiance du public par l'application des principes de transparence, le code source du logiciel électoral et tous les équipements et logiciels utilisés dans le système de vote électronique, y compris leur configuration, doivent être inscrits sur la liste des éléments à vérifier. Les protocoles liés aux opérations soumises à l'audit, tels que la procédure d'installation et de configuration, la vérification de l'adéquation entre le code source certifié et celui qui a été utilisé pendant l'élection, ainsi que la procédure de décompte des bulletins électroniques doivent également faire partie de la liste de vérification. Ces mesures devraient aider les États membres à fournir la documentation pertinente aux électeurs et à des tierces personnes, dont les observateurs nationaux et internationaux, et les médias.

L'expression « bien avant » implique de fixer dans la réglementation nationale des délais clairs pour la diffusion de ces informations, qui donnent aux acteurs concernés la possibilité d'en prendre connaissance, de réagir et de demander d'éventuelles modifications, ainsi que la possibilité d'exercer leurs droits. L'organisme en charge des élections devrait avoir le temps et la possibilité de prendre en compte ces retours d'information et d'y donner suite, par exemple en mettant à jour le système. Un délai de douze mois avant la date du scrutin semble indiqué pour satisfaire à l'exigence de diffusion de ces informations « bien avant » le début de la période électorale. Des délais plus courts pour les changements « de dernière minute » pourraient être nécessaires. Cela dit, les principaux éléments devraient être communiqués « bien avant » et non pas « peu de temps » avant l'élection.

c. Le déploiement des technologies de vote électronique devrait englober l'élaboration de lignes directrices complètes et détaillées, étape par étape, incluant un manuel de procédures.

32. Le public, en particulier les électeurs, sera informé bien avant le début du scrutin dans un langage clair et simple :
- de toutes les démarches qu'il pourrait avoir à effectuer pour y participer et voter ;
- de l'utilisation correcte et du bon fonctionnement du système de vote électronique ; et
- du calendrier du vote électronique, et de toutes ses étapes.

a. Des modalités d'aide et d'assistance concernant les procédures de vote devraient être mises à la disposition des électeurs.

Des modalités d'aide et d'assistance sur les procédures de vote devraient être disponibles quel que soit le mode de suffrage employé. Ces informations devraient être accessibles pour chacun des modes de suffrage électronique utilisés, au moins par la même voie. En d'autres termes, l'assistance devrait être accessible au minimum par le biais d'un site web et du courrier électronique dans le contexte du vote par internet, et, de la même manière, un système d'assistance téléphonique devrait être mis en place pour le vote par téléphone.

b. Pour le vote électronique à distance, les supports d'information à l'intention des électeurs devraient également être accessibles par un moyen de communication différent et généralement accessible.

Les informations sur le vote électronique à distance devraient également être accessibles sur un canal complémentaire, un moyen de communication, différent et généralement accessible en cas d'indisponibilité d'un mode de suffrage électronique à distance. Par exemple un service d'assistance téléphonique pourrait accompagner les systèmes de vote sur internet.

c. Les électeurs devraient se voir offrir la possibilité de s'exercer à l'utilisation de tout nouveau système de vote électronique avant le vote et indépendamment de celui-ci. Dans ce cas, l'attention des participants devrait être expressément attirée sur le fait que le scrutin auquel ils prennent part n'est pas une élection ou un référendum réel.

Les modes de suffrage traditionnels sont largement essayés et testés dans les États membres, et les électeurs connaissent bien les règles générales qui les régissent. L'introduction du vote électronique est un défi pour l'électeur, car la compréhension de ces systèmes et de leur fonctionnement n'est pas toujours aisée. Des mesures devraient donc être prises pour présenter les systèmes aux électeurs afin de maintenir le niveau de connaissance et de confiance du public. Ces mesures devront probablement s'inscrire dans la durée.

Pour accroître le niveau d'information et de confiance des électeurs à l'égard de tout (nouveau) système de vote électronique, il convient de leur donner la possibilité de s'exercer à l'utilisation de ces systèmes, avant un vote et indépendamment de celui-ci (par exemple au moyen de versions de démonstration ou par des élections test). Une attention particulière devrait être portée à cet égard aux catégories d'électeurs supposés rencontrer davantage de difficultés (par exemple les personnes âgées) et à leurs besoins spécifiques.

33. Les composantes du système de vote électronique seront divulguées à des fins de vérification et de certification.

a. Le système de vote électronique devrait générer des données d'observation fiables et suffisamment détaillées pour permettre l'observation du scrutin. Déterminer de manière fiable la date et l'heure à laquelle un événement a généré des données d'observation devrait être possible. L'authenticité, la disponibilité et l'intégrité des données devraient être assurées.

b. Les observateurs nationaux et internationaux devraient avoir accès à toute la documentation pertinente sur les processus de vote électronique.

Il est essentiel que les observateurs nationaux et internationaux aient accès à l'ensemble des documents pertinents et en particulier aux procès-verbaux et rapports de certification, de test et d'audit, ainsi qu'à une documentation technique détaillée expliquant le fonctionnement du système. Ces observateurs comprendront notamment des représentants des partis politiques et du grand public. Il convient de les inviter aux réunions qui les concernent. Dans la mesure du possible, les États membres, le fournisseur ou l'organe de certification devraient fournir des informations à toutes les parties prenantes, par exemple en mettant en ligne les documents utiles bien avant le début de la période électorale.

Les États membres devraient établir des procédures pour déterminer quelles parties prenantes ont accès à quels types d'informations, et à quel moment. Il conviendrait également de mettre au point de telles procédures pour les observateurs nationaux et internationaux, pour les médias ainsi que pour les autres acteurs concernés tels que les citoyens, les partis politiques et les ONG. Ces procédures devraient reposer sur le principe du libre accès.

Les États membres devraient clairement attirer l'attention des fournisseurs potentiels sur ces exigences ainsi que sur le fait que les différentes parties prenantes, et notamment les observateurs nationaux et internationaux, doivent avoir accès à certains documents pendant la période de l'appel d'offres. Tout accord de non-divulgation qui empêcherait les observateurs de publier les évaluations et les faits sur lesquels elles se basent priverait l'ensemble des parties prenantes, mais surtout les observateurs, d'informations importantes.

c. Les États membres devraient mettre la documentation pertinente à la disposition des observateurs, y compris, dans la mesure du possible, dans une langue communément utilisée dans les relations internationales.

Les informations nécessaires aux observateurs nationaux et internationaux pour mener à bien leurs travaux devraient être disponibles dans la ou les langue(s) officielle(s) du pays concerné. Ces informations devraient, dans la mesure du possible, être également mises à disposition dans l'une des langues officielles du Conseil de l'Europe (anglais et français), ces versions linguistiques étant notamment demandées par les observateurs internationaux.

d. Les États membres devraient mettre en place des programmes de formation destinés aux groupes d'observateurs nationaux et internationaux.

Pour les non-initiés, le fonctionnement des systèmes de vote électronique peut être difficile à appréhender. Des formations devraient donc être proposées, en particulier aux observateurs nationaux et internationaux, pour améliorer leur compréhension du système utilisé. Celles-ci leur apporteraient des outils élémentaires et faciles à utiliser lors des travaux d'observation, outils qui incluraient des méthodes pour contrôler le scellement, lire les impressions des machines à voter et lire les fichiers d'audit.

e. Les observateurs nationaux et internationaux, et les médias devraient pouvoir observer les tests pratiqués sur les logiciels et équipements de vote.

Les différentes parties prenantes, notamment les groupes d'observateurs accrédités, devraient non seulement avoir accès à la documentation, mais aussi pouvoir contrôler la vérification des dispositifs et systèmes de vote électronique. L'observation de ces tests et/ou audits ne devrait pas gêner la conduite des élections. Par conséquent, elle ne devrait se dérouler que sous la direction des personnes chargées de l'organisation de ces élections. Comme cela a déjà été mentionné, ces observateurs devraient notamment comprendre des représentants des partis politiques et du grand public. Par ailleurs, les personnes chargées de l'observation des tests et/ou audits devraient avoir suivi une formation préalable. Le processus devrait se dérouler de façon suffisamment ouverte pour que les observateurs puissent évaluer pleinement le fonctionnement du dispositif.

f. Les observateurs électoraux devraient avoir accès à toutes les phases du processus d'évaluation et de certification.

Ces vingt dernières années, l'observation des élections s'est révélée être un excellent moyen d'assurer la transparence électorale et l'accès aux processus électoraux. L'avènement du vote électronique impose toutefois une modernisation des méthodes en vigueur dans ce domaine. Pour permettre aux observateurs de suivre les processus de certification des systèmes de vote électronique, il faudra prolonger la durée des missions d'observation électorale. Il est essentiel

qu'aucune procédure de certification du vote électronique ne se déroule à huis clos, car cela ferait inévitablement naître des soupçons.

Les observateurs, y compris les représentants des partis politiques et le grand public, devraient avoir accès à l'ensemble des informations pertinentes pendant toute la durée du processus de certification, afin de pouvoir accomplir correctement leur mission. Les observateurs devront pour leur part expliciter leur méthodologie.

VII. Lignes directrices pour la mise en œuvre des recommandations sur la responsabilité

36. Les États membres élaboreront des exigences techniques, d'évaluation et de certification, et veilleront à ce que ces exigences soient totalement conformes aux principes juridiques et démocratiques pertinents. Les États membres tiendront les exigences à jour.

a. Les États membres devraient établir les objectifs du processus de certification et les méthodes de certification.

Lorsque l'on envisage la certification d'un système de vote électronique – qu'il fonctionne ou non à distance –, la première étape consiste à définir clairement les objectifs et les exigences de la procédure de certification. Pour définir ces exigences, il importe de vérifier si elles sont conformes à la législation nationale et aux normes internationales en vigueur, y compris en ce qui concerne les procédures d'appel ou de dépôt de plainte concernant la conduite des élections. Si la définition d'un ensemble d'exigences très précises peut apparaître, a priori, comme une option satisfaisante pour garantir une bonne analyse en vue de la certification, un tel cadre juridique peut – du fait de son caractère rigide – avoir des effets pervers. Par exemple, les contrôleurs des systèmes seraient alors soumis à des exigences très strictes tandis que les concepteurs et fournisseurs des systèmes en question n'auraient qu'à adapter leurs produits aux exigences particulières de telle ou telle administration électorale. Cela ne les inciterait pas à améliorer davantage leur produit et l'administration électorale concernée serait dès lors contrainte, du fait des règles juridiques qu'elle a elle-même fixées, d'accepter un produit qui ne serait pas d'une qualité optimale. Le recours à un contrat dans lequel le critère de sélection serait la qualité et non le prix devrait contribuer à éviter ce piège.

Le fait de préciser les objectifs poursuivis et les besoins en termes de logiciel, de système d'exploitation, de matériel et le processus de vote électronique, et l'étendue de la certification et ses méthodes pourra contribuer à l'efficacité du processus de certification, à l'utilisabilité du système de certification et à la transparence globale des systèmes de vote électronique.

Le processus de certification des systèmes de vote électronique ne se limite pas à la certification initiale; il recouvre également une démarche de « décertification » et de « recertification » des logiciels, des systèmes d'exploitation, des matériels et des processus.

La confiance du citoyen peut être conditionnée par un certain nombre de facteurs sociopolitiques qui peuvent poser problème. Ces facteurs pouvant avoir des incidences sur les processus de certification, les États membres devraient développer la recherche scientifique dans ce domaine, y compris par des échanges, au niveau international, d'informations pertinentes.

Il conviendrait de mettre en place une structure qui permette de faire en sorte que toutes les parties concernées connaissent et comprennent bien le système utilisé. Tous les efforts déployés dans ce domaine devraient se fonder sur des méthodologies bien établies comme les tests de confirmation, les tests de composants, les tests de performance et les tests de fonctionnement.

37. Avant la mise en service de tout système de vote électronique, et à intervalles réguliers par la suite, en particulier si des changements substantiels ont été apportés au système, un organisme indépendant et compétent évaluera la conformité de ce système et de tout composant de technologies de l'information et de la communication (TIC) avec les exigences techniques. Cela peut prendre la forme d'une certification formelle ou d'un autre contrôle approprié.

a. Les États membres devraient déterminer la répartition des coûts liés au processus de certification. Ils devraient définir la responsabilité, y compris financière, de l'organe de certification en ce qui concerne la qualité de ses travaux.

Quiconque autorisé à participer au processus de certification d'un système de vote électronique – y compris les certificateurs, les évaluateurs et les contrôleurs – doit être indépendant et qualifié. Les critères, modalités et institutions compétentes impliquées dans la sélection des organes de

certification devraient par conséquent être expressément mentionnés dans la législation nationale, de même que les instances chargées de cette sélection. Il incombe aux États membres de définir les règles et directives correspondantes.

Les procédures applicables doivent être connues et rendues publiques bien avant la date des élections. Cela facilitera la tâche des fournisseurs de systèmes et les électeurs seront ainsi plus confiants dans les procédures en question. Le nombre d'organes de certification potentiels ne devrait pas être restreint. Quiconque étant indépendant et réunissant les conditions requises devrait pouvoir participer au processus de sélection. Une consultation publique ou un appel d'offres européen avec plusieurs soumissionnaires seraient à privilégier pour désigner ceux qui réaliseront les opérations de certification.

Les États membres devraient envisager de confier la sélection des organes de certification à des contrôleurs professionnels certifiés au niveau international. La certification « CISA » (« Certified Information System Auditors ») en est un exemple : elle reconnaît les compétences professionnelles de ceux qui contrôlent, surveillent et évaluent les systèmes de technologie de l'information et les systèmes administratifs des organisations. Une attention particulière devrait être portée au coût de ces procédures. Autre élément important : le recours à des certificats internationaux ne devrait pas devenir un obstacle empêchant les États membres d'utiliser un système de vote électronique donné, voire d'utiliser un système de vote électronique valide.

Les États membres devraient préciser d'entrée de jeu quel organisme prendra en charge le coût de la procédure de certification. Ils pourront décider que la totalité des coûts, y compris ceux de la certification officielle, sera à la charge des fournisseurs, ce qui pourrait se traduire par un engagement plus important de ces derniers. Une autre possibilité serait de faire supporter l'ensemble des coûts à l'État membre, la troisième solution étant le partage des coûts. Le coût de la certification ne devrait en aucun cas compromettre l'indépendance, l'intégrité et la qualité du processus. Quelle que soit l'option retenue, chaque État membre devrait disposer de crédits suffisants pour la certification et rendre la décision publique.

b. Les organismes d'évaluation et de certification devraient disposer d'un accès complet à l'ensemble des informations pertinentes et se voir accorder suffisamment de temps pour pouvoir mener à bien le processus de certification avant l'élection.

Les organismes chargés de la certification devraient avoir accès aux informations et aux données nécessaires et suffisantes pour l'accomplissement de leur mission – c'est-à-dire la formulation de conclusions sur le système de vote électronique examiné ; ils devraient avoir suffisamment de temps pour passer en revue l'ensemble des informations et données. Les citoyens ont le droit de savoir quel type d'informations n'ont pas été jugées nécessaires et suffisantes pour être utilisées dans le processus de certification. En outre, les règles régissant la relation entre le vendeur et le certificateur, telles que les accords de confidentialité et documents similaires, devraient être rendues publiques.

Dans certains cas, notamment lors d'élections anticipées ou de l'introduction d'un nouveau système de vote, le processus de certification peut n'avoir été engagé que peu de temps avant l'ouverture des élections. Le risque est alors de manquer de temps pour procéder à une certification plus poussée, compromettant ainsi la crédibilité du scrutin. Le processus de certification devrait donc être achevé avant la date des élections, afin de laisser suffisamment de temps pour en examiner les conclusions.

Pour résoudre ce problème et économiser du temps et de l'argent, on pourrait envisager de procéder à une certification initiale du système de vote électronique, puis, pour la certification ultérieure, de ne certifier que les modules modifiés et leur séquence. Cela nécessite toutefois d'établir une distinction entre les changements majeurs (modification) et les changements mineurs du système de vote électronique.

c. Le mandat de l'organe d'évaluation et de certification devrait être confirmé à intervalles réguliers.

Les États membres devraient établir des procédures non seulement pour la sélection initiale des organes de certification, mais également pour le réexamen de leur mandat et les décisions de confirmation ou de non-reconduction de celui-ci. Tout mandat d'un organe de certification des systèmes de vote électronique devrait être accordé pour une durée limitée. De nouveaux appels d'offres doivent avoir lieu à intervalles réguliers et être rendus publics. Il convient d'établir clairement si la décision de confier le processus de certification à tel ou tel organisme relève du fournisseur ou des autorités électorales compétentes.

d. Les informations contenues dans le rapport de certification devraient servir à établir les conclusions de ce dernier.

Les rapports de certification du rapport de certification ne devraient pas reposer sur d'autres informations que celles qu'il contient de manière à ce qu'une tierce partie puisse réenquêter sur ces bases et confirmer la validité des conclusions.

e. Dans un souci de transparence, les États membres devraient fixer et publier des règles claires en matière de communication du rapport final de certification et de tout autre document pertinent. *Les États membres devraient établir et publier des consignes permettant de déterminer qui a accès à quelles informations, et à quel moment. Une attention toute particulière doit être accordée aux besoins des observateurs nationaux et internationaux, ainsi qu'à ceux des médias. Il convient de prévoir également des règles concernant les autres parties prenantes : citoyens, partis politiques, ONG et, à tout le moins, aux membres du personnel électoral. Ces règles sont indispensables pour renforcer la confiance des citoyens dans la sécurité et la fiabilité des systèmes de vote électronique, ainsi que dans la fonction de contrôle qu'exercent les autorités électorales. Ce n'est que dans des circonstances exceptionnelles que l'on pourra envisager de ne pas divulguer le rapport de certification ou certaines parties du rapport ou d'autres documents pertinents.*

Il faudra accorder une attention particulière aux éléments du logiciel nécessaires à la sécurité du système, par exemple en incluant des tests de sécurité dans les plans de test et d'évaluation pour que le lecteur sache comment il a été procédé aux vérifications de sécurité du système. On pourra également envisager un marquage de l'ensemble des documents par les États membres et les fournisseurs.

Les fournisseurs de systèmes, et quelquefois, les certificateurs eux-mêmes, peuvent s'opposer à la publication de certaines parties, voire de la quasi-totalité, des documents relatifs au système de vote électronique, dans un souci de protection des droits de la propriété intellectuelle. Si l'on veut éviter que le processus de certification ne soit entouré d'un trop grand secret, il faudra sensibiliser les fournisseurs et certificateurs potentiels, dans le cadre de l'appel d'offres, au fait que tous les acteurs concernés doivent avoir accès à certains documents. Tout accord de non-divulgation qui empêcherait les observateurs de publier leurs évaluations et les faits sur lesquels elles reposent nuirait à l'efficacité de la mission d'observation.

Enfin, pour superviser le processus de certification ou compenser toute publication partielle ou incomplète des informations au public, les États membres pourraient créer des comités spéciaux composés d'experts, d'universitaires et/ou de responsables politiques. Par exemple, il existe en Belgique un collège d'experts chargé de superviser l'ensemble du processus électoral pour l'assemblée législative compétente.

39. Le système de vote électronique pourra faire l'objet d'un audit. Le système d'audit sera ouvert et complet, et signalera effectivement les menaces et les problèmes potentiels.

a. Il conviendrait d'enregistrer dans le système d'audit les dates et heures et les événements et actions, notamment :

- toutes les informations relatives au scrutin, y compris le nombre d'électeurs admissibles, le nombre de suffrages exprimés, le nombre de votes valides et nuls, les dépouillements et nouveaux décomptes, etc. ;
- toute attaque contre le système de vote électronique et ses infrastructures de communication ;
- les pannes, dysfonctionnements et autres menaces contre le système.

Les outils automatisés et les procédures du système devraient permettre une procédure rapide et précise d'analyse des données et d'élaboration des rapports y relatifs, afin que les mesures correctives puissent être prises sans tarder. Le système d'audit devrait fournir des rapports vérifiables sur :

- *les recoupements (vérifications croisées) de données ;*
- *les attaques contre le système ou le réseau ;*
- *la détection d'intrusions et les rapports correspondants ;*
- *les manipulations de données ;*
- *les fraudes et tentatives de fraude.*

Le système d'audit devrait conserver le relevé de toutes les attaques contre le système électoral ou référendaire ou son infrastructure de communication. Le système comportera un dispositif permettant de détecter et de faire rapport sur toutes les tentatives de piratage, d'intrusion ou de manipulation.

Toute attaque contre le système de vote doit, une fois détectée, être consignée, signalée et donner lieu à une réaction immédiate.

Le système d'audit devrait établir le relevé de tous les décomptes et nouveaux décomptes, y compris les décisions et mesures prises, ainsi que les exceptions faites pendant le dépouillement.

b. Le système de vote électronique devrait être doté d'horloges synchronisées fiables. La précision de ce système d'horodatage devrait être suffisante pour conserver des repères temporels pour les journaux d'audit et les données d'observation, ainsi que les délais d'inscription, de nomination, de vote ou de dépouillement.

La précision nécessaire peut varier suivant les utilisateurs de la source de synchronisation ; il peut y avoir par exemple des tolérances différentes pour l'inscription des électeurs et l'enregistrement des suffrages. L'on peut donc envisager de mettre en place une ou plusieurs sources de synchronisation, ou une seule offrant la plus grande précision. L'expression « repère temporel » est utilisée pour indiquer que les données sont marquées. Il existe plusieurs moyens de le faire, selon la situation envisagée : le système peut recourir à des marquages temporels inviolables pour les événements sensibles, tandis que des séquences continues de chiffres ou la préservation de la séquence, par exemple, pourraient suffire dans les entrées de journal. On notera toutefois que des marquages temporels sur les suffrages peuvent compromettre la confidentialité du scrutin. C'est pourquoi il faudrait examiner avec soin s'il est opportun d'y recourir, et de quelle manière, pour les bulletins ou les suffrages.

c. Les conclusions de l'audit devraient être prises en compte pour la préparation des élections électroniques ultérieures.

VIII. Lignes directrices pour la mise en œuvre des recommandations relatives à la fiabilité et à la sécurité du système

40. L'administration électorale sera responsable du respect et de l'application de toutes les exigences même en cas de défaillances et d'attaques. L'administration électorale sera responsable de la disponibilité, de la fiabilité, de la capacité effective d'utilisation et de la sécurité du système de vote électronique.

a. La disponibilité des services de vote électronique pour tous les électeurs durant toute la procédure de vote électronique est préservée.

Tout système de vote électronique devrait être protégé contre les pannes et les dysfonctionnements. Toutefois, on ne peut jamais exclure entièrement l'éventualité d'une panne. Des procédures et des solutions alternatives devraient être prévues en cas d'urgence.

b. Les électeurs devraient être informés rapidement, par les moyens appropriés, de toute interruption, de toute suspension ou de tout redémarrage du système de vote électronique.

c. Le système de vote n'exclut pas du vote des électeurs admissibles.

d. Le système de vote électronique devrait préserver la disponibilité et l'intégrité des suffrages.

Dès lors que le suffrage a été enregistré, personne ne devrait plus être en mesure de le lire, de le modifier ou de le relier à l'électeur qui l'a exprimé. C'est le but de l'opération consistant à sceller l'urne, et à sceller le bulletin durant son transfert de l'électeur à l'urne dans le contexte du vote à distance. Dans certaines conditions, le scellement est effectué au moyen d'un cryptage.

Le scellement d'une urne requiert des mesures physiques et organisationnelles. Celles-ci englobent le verrouillage physique de l'urne et sa surveillance par plus d'une personne. En présence d'une urne électronique, des mesures complémentaires sont nécessaires, tels des contrôles d'accès, des structures d'autorisation et des pare-feu.

Un bulletin est scellé dès lors que les mesures permettant de faire en sorte qu'il ne puisse être ni lu, ni modifié, ni relié à l'électeur qui l'a émis ont été appliquées à son contenu.

Les accords de niveau de service (Service level agreements – SLA) fixent généralement des taux de disponibilité et de défaillance. Un certain niveau de dégradation de service peut être admissible pendant les périodes de dérangement, par exemple quand un serveur d'une grappe tombe en panne. Pendant les processus d'inscription, même de brèves interruptions de service ou des périodes de maintenance peuvent être acceptables.

Le concepteur du système devrait toutefois envisager l'éventualité d'attaques délibérées par saturation et devrait donner des informations sur les réserves de moyens prévues pour maintenir le fonctionnement du système. La réalisation de tests d'intrusion indépendants peut diminuer la probabilité de réussite d'une perturbation délibérée contre le système.

Le choix des services dont la disponibilité doit être préservée dépend de la période concernée – préélectorale, électorale et postélectorale. En période préélectorale, les opérations qui doivent être accessibles sont la nomination des candidats et l'inscription des électeurs et les services correspondants ; en période électorale, ce sont le vote et les services correspondants ; et, en période postélectorale, le dépouillement et la communication des résultats et les services correspondants. Il doit exister des processus d'audit à toutes les étapes. Les limites d'acceptabilité prédéfinies pour les contrats de niveau de service, les taux de défaillance ou les dégradations de service peuvent toutefois varier selon les étapes ou les services concernés.

e. Des mesures techniques et organisationnelles devraient être prises pour empêcher toute perte définitive de données en cas de panne ou de défaut affectant le système de vote électronique.

f. Les États membres devraient prêter une attention particulière à l'utilisabilité dans la conception des dispositifs de sécurité.

Lignes directrices 40e et 40f : Cela ne signifie pas que toutes les méthodes de protection disponibles doivent être utilisées. Il convient de déterminer dans chaque cas la nature et l'étendue des mesures de protection à appliquer, et d'établir un juste équilibre entre certains aspects différents, mais de même importance, par exemple entre l'impératif sécuritaire et la volonté de disposer d'un système facile à utiliser par les électeurs. En pareil cas, le souci d'assurer la commodité d'utilisation ne doit pas l'emporter sur la nécessité de garantir un haut niveau de sécurité, mais peut constituer un élément dans le choix des mesures de sécurité à adopter. Les mêmes considérations peuvent s'appliquer dans une situation où l'on privilégierait une amélioration minime de la sécurité au détriment de l'utilisabilité.

g. Des vérifications régulières devraient être effectuées pour s'assurer de la conformité des éléments du système de vote électronique à ses spécifications techniques et de la disponibilité de ses services.

h. Les équipements clés du suffrage électronique devraient être situés dans une zone sécurisée, qui sera protégée en permanence contre toute intrusion ou tout accès non autorisé pendant la période de l'élection ou du référendum.

i. Un plan de restauration après sinistre devrait être mis en œuvre pendant la période de l'élection ou du référendum.

Lignes directrices 40h et 40i : Pour leur sécurité, il est particulièrement souhaitable que les systèmes centraux soient installés dans des lieux protégés et placés sous surveillance. L'accès physique devrait en être contrôlé et restreint. Pour pouvoir réagir en cas de dégâts matériels, il faudrait prévoir un lieu de substitution dans lequel l'équipement adéquat aura été mis en réserve (plan de secours).

Les autorités électorales devront définir le niveau de service attendu avant de mettre en route le système. Suivant le niveau à atteindre, il pourrait être nécessaire de réaliser une analyse des risques et de mettre au point des scénarios. Cela implique des procédures, des dispositifs de sauvegarde, des protocoles de réservation de ressources, etc.

j. Il devrait être possible de vérifier à tout moment l'état de protection des équipements de vote. Les responsables de l'équipement devraient utiliser des procédures de contrôle spéciales pour garantir, pendant le déroulement du scrutin, la conformité des équipements de vote et de leur utilisation aux exigences requises.

k. Des dispositifs de secours suffisants devraient être mis en place et disponibles en permanence pour assurer un déroulement sans heurts du scrutin. Tout système de secours devrait répondre aux mêmes normes et exigences que le système d'origine.

l. Le personnel concerné devrait être prêt à intervenir rapidement selon une procédure établie par les autorités électorales compétentes.

i. Les personnes responsables du fonctionnement des équipements devraient établir une procédure d'urgence.

ii. Toute opération technique devrait être soumise à une procédure officielle de contrôle. Tout changement important apporté à un équipement clé devrait être notifié.

Lignes directrices 40j, 40k et 40l : Les systèmes de vote électronique nécessitent des procédures formalisées pour contrôler leur sécurité et leur fiabilité, ainsi que des procédures et des moyens suffisants pour la résolution des problèmes touchant l'infrastructure.

Les autorités électorales devraient avoir connaissance de tous les changements importants apportés au système afin d'anticiper toutes les conséquences qu'elles pourraient avoir et de réfléchir à la méthode la plus appropriée pour communiquer ces changements.

m. Toutes les données conservées après la période de l'élection ou du référendum devraient être stockées en lieu sûr.

Toutes les données relatives aux élections ou aux référendums qui doivent être conservées devraient l'être de manière sécurisée, ce qui implique de réaliser plusieurs copies des données sur différents types de supports (disque dur, sauvegarde sur bande, médias optiques tels que les DVD ou microfiches, clé USB, version papier) et de les stocker en plusieurs endroits.

41. Seules les personnes autorisées par l'administration électorale auront accès à l'infrastructure centrale, aux serveurs et aux données relatives à l'élection. La nomination des personnes autorisées à gérer le vote électronique sera clairement réglementée.

a. Ces personnes auront un accès restreint aux services de vote électronique, en fonction de leur identité ou de leur rôle d'utilisateur. L'authentification de l'utilisateur devrait être assurée avant toute action. La séparation des tâches devrait être claire et strictement assurée au moyen de mesures techniques.

b. Pendant l'ouverture de l'urne électronique, toute intervention autorisée touchant le système devrait être réalisée par des équipes d'au moins deux personnes, faire l'objet d'un compte rendu et être contrôlée par des représentants de l'administration électorale et par tout observateur électoral.

c. Toute autre intervention technique sensible devrait être réalisée par des équipes d'au moins deux personnes. La composition de ces équipes devrait changer régulièrement. Dans la mesure du possible, ces interventions devraient être réalisées en dehors des périodes électorales. Elles devraient faire l'objet d'un compte rendu.

42. Avant toute élection électronique, l'administration électorale devra s'assurer que le système de vote électronique est authentique et qu'il fonctionne correctement.

a. Avant chaque scrutin, l'équipement devrait être vérifié et approuvé conformément à un protocole établi par les autorités électorales compétentes. L'équipement devrait être vérifié afin de garantir sa conformité aux spécifications techniques. Les conclusions de cette vérification devraient être soumises aux autorités électorales compétentes.

Il convient de distinguer les contrôles effectués régulièrement après chaque élection ou référendum et les contrôles réalisés chaque fois que le système subit un changement, quel qu'il soit. Dans le premier cas, les vérifications pourraient être confiées au personnel de l'entité qui exploite le système d'élection ou de référendum électronique, tandis que, dans le deuxième cas, c'est une instance externe qui devrait s'en charger, cette procédure relevant davantage de l'homologation.

43. Une procédure sera établie pour l'installation régulière des mises à jour et des corrections de tous les logiciels concernés.

a. Des procédures formelles devraient être établies pour le déploiement des logiciels et la configuration des technologies de vote. Des délais devraient être définis pour les mises à jour. Les mises à jour distribuées devraient être authentifiées (signées).

46. L'administration électorale manipulera tout le matériel crypté de manière sécurisée.

a. Les clés privées de cryptographie devraient être générées lors d'une réunion publique et elles devraient être séparées en plusieurs parts et partagées au moins par deux personnes dont il est peu probable qu'elles soient de connivence.

47. En cas d'incident susceptible d'affecter l'intégrité du système, les personnes chargées du fonctionnement de l'équipement en informeront immédiatement l'administration électorale.

a. Les autorités électorales définiront au préalable les types d'incidents à signaler.

b. En cas d'incidents, les autorités électorales compétentes devraient prendre les mesures nécessaires pour atténuer les effets de cet incident.

48. L'authenticité, la disponibilité et l'intégrité des listes électorales et des listes de candidats seront préservées. L'origine des données sera authentifiée. Les dispositions relatives à la protection des données seront respectées.

a. L'impression des données d'identification des électeurs, comme celles figurant sur les cartes d'électeurs, devrait être contrôlée afin de garantir la sécurité des données sensibles.

49. Le système de vote électronique identifiera les suffrages qui sont entachés d'irrégularité.

a. Il devrait être possible d'établir qu'un suffrage a été exprimé dans les délais prescrits.

Dans le contexte d'un vote par internet, l'expression « dans les délais prescrits » désigne le dernier délai avant la clôture du scrutin sur internet. Cette exigence peut être mise en œuvre par horodatage ou par une confirmation au moyen d'un système fiable. Les informations d'horodatage ne devraient toutefois pas être utilisées pour révéler le contenu du vote.

ANNEXE

Glossaire

Aux fins des présentes lignes directrices, les termes suivants sont ainsi définis :

- accord de non-divulgation : contrat juridique entre deux parties au moins, précisant les éléments, les données ou informations confidentiels que les différentes parties en question souhaitent partager à des fins précises, mais en n'autorisant qu'un accès restreint aux parties extérieures au contrat ;
- administration électorale : institution chargée de gérer les élections dans un pays donné ou à un niveau national ou inférieur ;
- authentification : apport d'une garantie de l'identité déclarée d'une personne ou d'une garantie des données ;
- bulletin de vote : moyen juridiquement reconnu par lequel l'électeur peut exprimer son vote ;
- candidat : option de vote consistant en une personne, un groupe de personnes et/ou un parti politique ;
- certificat : document publié à l'issue d'un processus officiel de certification – qui certifie ou approuve un fait ;
- certification : processus visant à confirmer la conformité d'un système de vote électronique avec les exigences et les normes prescrites, et prévoyant au minimum des dispositions en vue d'attester du bon fonctionnement du système. Ce processus peut aller d'un simple test ou contrôle jusqu'à une certification officielle. Il en résulte un rapport et/ou un certificat ;
- certification officielle : certification menée sous l'égide des autorités officielles, avant le jour du scrutin, et permettant de délivrer un certificat ;
- chaîne de confiance : processus de sécurité informatique, qui consiste à valider chaque composante du matériel et du logiciel utilisés selon une approche globale. Ce processus permet de s'assurer, tout en conservant une certaine souplesse, que seuls sont utilisés du matériel et des logiciels sûrs ;
- confidentialité : le fait de ne pas laisser d'informations disponibles ou de ne pas les divulguer à des personnes, des entités ou des processus non autorisés ;
- contrôle (ou audit) : évaluation indépendante, avant ou après une élection, d'une personne, organisation, système, processus, entité, projet ou produit, qui inclut des analyses quantitatives et qualitatives ;
- contrôle d'accès : prévention de toute utilisation non autorisée d'une ressource ;
- disponibilité : le fait d'être accessible et utilisable sur demande ;
- électeur : personne habilitée à exprimer un suffrage dans une élection ou un référendum donné ;
- élection électronique : élection ou référendum politique ayant recours au vote électronique ;
- enregistrement du suffrage : insertion du vote dans l'urne ;
- environnement contrôlé : locaux supervisés par du personnel électoral, par exemple bureau de vote, ambassade ou consulat ;
- évaluation : évaluation de personnes, de matériels, de logiciels et des procédures de vérification de leur adéquation à l'accomplissement de certaines tâches ;
- exigence : exposé documenté de la nature ou des objectifs d'un produit ou d'un service particulier ;
- libre accès : accès en ligne à différents matériels qui peuvent être lus et éventuellement utilisés (ou réutilisés) librement par tous dans certaines limites ;
- lignes directrices : tout document visant à rationaliser un ensemble de procédures très précises, selon des règles établies. Par définition, les lignes directrices ne sont pas juridiquement contraignantes ;
- liste électorale : liste des personnes habilitées à voter (électeurs) ;
- mode de suffrage : moyen par lequel un électeur peut exprimer son vote ;
- norme (juridique) : désigne les dispositions de l'Annexe I à la Recommandation CM/Rec(2017)5 ;
- norme (technique) : toute norme établie sous forme de document officiel définissant les critères techniques et de gestion, les méthodes, les processus et les pratiques qui doivent être communs à tous ;
- options de vote : éventail des possibilités parmi lesquelles un choix peut être effectué par l'expression d'un suffrage lors d'une élection ou d'un référendum ;
- organe de certification (ou « certificateur ») : organisme habilité à effectuer un processus de certification et à délivrer un certificat au terme de ce processus ;
- partie prenante : tout(e) personne, groupe, organisation ou système ayant un impact sur les actions d'un gouvernement ou d'une organisation, ou concerné(e) par ces actions. Les parties prenantes comprennent les citoyens, les administrateurs d'élections, les partis politiques, les gouvernements, les observateurs nationaux et internationaux, les médias, les universitaires, les ONG ou OING, les groupes d'opposants au vote électronique et les organismes spécifiques chargés de la certification du vote électronique ;
- profil de protection : ensemble d'exigences de sécurité, indépendant de l'application, pour une catégorie de produits qui couvre les besoins de sécurité spécifiques des utilisateurs ;
- rapport de certification : document exposant les éléments approuvés par un certificat, ainsi que le mode de certification ;
- sceller : protéger l'information, notamment par cryptage, afin qu'elle ne puisse être utilisée ou interprétée sans l'aide d'autres informations ou moyens dont ne disposent que des personnes ou autorités spécifiques ;

- suffrage électronique : suffrage enregistré par des moyens électroniques ;
- système de vote électronique : matériels, logiciels et procédures permettant de voter par voie électronique lors d'une élection ou d'un référendum ;
- test : vérification du bon fonctionnement des éléments étudiés ;
- test des composants et composantes : mode de contrôle de chaque unité individuelle du système de code, afin de déterminer sa validité ;
- urne électronique : moyen électronique par lequel les suffrages sont stockés dans l'attente du dépouillement ;
- vote : expression du choix parmi des options de vote ;
- vote électronique : utilisation de moyens électroniques pour enregistrer et/ou dépouiller les suffrages ;
- vote électronique à distance : utilisation de moyens électroniques pour exercer son suffrage en dehors des locaux où le vote se déroule en général.