Les normes juridiques, opérationnelles et techniques relatives au vote électronique

Recommandation Rec(2004)11
adoptée par le Comité des Ministres
du Conseil de l'Europe
le 30 septembre 2004
et exposé des motifs

Editions du Conseil de l'Europe

Edition anglaise :

Legal, operational and technical standards for e-voting
(Recommendation Rec(2004)11 and explanatory memorandum)
ISBN 92-871-5635-2

Editions du Conseil de l'Europe
F-67075 Strasbourg Cedex

ISBN 92-871-5634-4

Imprimé dans les ateliers du Conseil de l'Europe

1. Recommandation Rec(2004)11, adoptée par le Comité des Ministres du Conseil de l'Europe le 30 septembre 2004, et préparée par le Groupe ad hoc multidisciplinaire de spécialistes sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (IP1-S-EE).

2. La présente publication contient également l'exposé des motifs.

Recommandation Rec(2004)11

du Comité des Ministres aux Etats membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique

(adoptée par le Comité des Ministres le 30 septembre 2004, lors de la 898e réunion des Délégués des Ministres)

Le Comité des Ministres, agissant 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 dans le but de préserver et de promouvoir ses idéaux et principes, qui sont leur patrimoine commun ;

Réaffirmant sa conviction du fait que la démocratie représentative et directe fait partie de ce patrimoine commun et 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 ;

Respectant 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 la discrimination à l'égard des femmes ;

– 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) ;

– la Recommandation n° R (99) 5 du Comité des Ministres sur la protection de la vie privée sur Internet ;

– 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 ; et

– 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 ;

Ayant à l'esprit que le droit de vote est l'un des principaux fondements de la démocratie et que les procédures des systèmes de vote électronique doivent par conséquent être conformes aux principes relatifs au déroulement des élections et référendums démocratiques ;

Reconnaissant que, face au recours croissant aux nouvelles technologies de l'information et de la communication dans la vie quotidienne, les Etats membres devraient prendre en compte cette évolution dans leurs procédures démocratiques ;

Notant que les élections et référendums aux niveaux local, régional et national se caractérisent dans certains Etats membres par un taux de participation faible, voire en diminution constante ;

Notant que certains Etats membres utilisent déjà ou 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 à l'électeur l'enregistrement de son suffrage ;

– faciliter la participation aux élections et référendums de toutes les personnes autorisées à voter, et en particulier des citoyens résidant ou séjournant à l'étranger ;

– étendre l'accès au scrutin aux 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 pour la communication et la participation à la vie civique afin de faire progresser la démocratie ;

– réduire progressivement le coût global pour les autorités électorales de l'organisation d'élections ou d'un référendum ;

– 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 ;

Conscient des inquiétudes que suscitent divers problèmes de sécurité et de fiabilité que pourraient poser certains 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 la confiance du public nécessaire à l'organisation d'élections électroniques,

Recommande aux gouvernements des Etats membres qui recourent au vote électronique ou envisagent d'y recourir de se conformer, sous réserve du paragraphe iv ci-dessous, aux paragraphes i à iii ci-dessous, aux normes et exigences juridiques, opérationnelles et techniques du vote électronique, telles qu'elles figurent dans les annexes à la présente recommandation :

i. le vote électronique doit respecter tous les principes des élections et référendums démocratiques ; il doit être aussi fiable et sûr que les élections et référendums démocratiques qui n'impliquent pas le recours aux moyens électroniques. Ce principe général s'applique à tous les aspects des élections, qu'ils soient ou non mentionnés dans les annexes ;

ii. l'interconnexion des aspects juridiques, opérationnels et techniques du vote électronique, tels qu'ils sont présentés dans les annexes, doit être prise en compte dans la mise en œuvre de cette recommandation ;

iii. les Etats membres devraient envisager de passer en revue leurs dispositions législatives pertinentes à la lumière de cette recommandation ;

iv. les principes et dispositions énoncés dans les annexes de la présente recommandation n'exigent cependant pas de chaque Etat membre qu'il modifie les procédures de vote internes en application au moment de l'adoption de cette recommandation, qui peuvent être conservées en cas d'utilisation du vote électronique, du moment que ces procédures respectent tous les principes des élections et référendums démocratiques ;

v. afin de fournir au Conseil de l'Europe une base à partir de laquelle il pourra élaborer les actions futures en matière de vote électronique dans les deux ans après l'adoption de cette recommandation, le Comité des Ministres recommande que les Etats membres :

– assurent un suivi de leur politique et de leur expérience en matière de vote électronique, et en particulier de la mise en œuvre des dispositions de cette recommandation ; et

– acceptent de faire rapport au Secrétariat du Conseil de l'Europe sur les conclusions de leurs analyses, qui les communiquera aux Etats membres et assurera le suivi de la question du vote électronique.

Aux fins de la présente recommandation, les termes suivants sont ainsi définis :

– authentification : apport d'une garantie de l'identité déclarée d'une personne ou de données ;

– bulletin de vote : moyen juridiquement reconnu par lequel l'électeur peut exprimer son choix parmi les options de vote ;

– candidat : option de vote consistant en une personne, un groupe de personnes et/ou un parti politique ;

– électeur : personne habilitée à exprimer un suffrage dans une élection ou un référendum donné ;

– élection ou référendum électronique : élection ou référendum politique ayant recours à des moyens électroniques lors d'une ou de plusieurs étapes ;

– enregistrement du suffrage : insertion du vote dans l'urne ;

– liste électorale : liste des personnes habilitées à voter (électeurs) ;

– mode de suffrage : moyen par lequel un électeur peut exprimer son vote ;

– 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 ;

– sceller : protéger l'information 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 ;

– urne électronique : moyen électronique par lequel les suffrages sont stockés dans l'attente du dépouillement ;

– vote : expression du choix parmi les options de vote ;

– vote électronique : élection ou référendum électroniques qui impliquent le recours à des moyens électroniques au moins lors de l'enregistrement du suffrage ;

– vote électronique à distance : vote électronique où le suffrage est enregistré au moyen d'un dispositif non contrôlé par une autorité électorale.

Annexe I

Normes juridiques

A. Principes

I. Suffrage universel

1. L'interface utilisateur du système de vote électronique sera compréhensible et facilement utilisable.

2. Les éventuelles procédures d'inscription au vote électronique ne constitueront pas un obstacle empêchant l'électeur de participer au vote électronique.

3. Les systèmes de vote électronique seront, dans toute la mesure du possible, conçus de manière à maximiser les possibilités qu'ils peuvent offrir aux personnes handicapées.

4. A moins que les modes de vote électronique à distance ne soient universellement accessibles, ils ne constitueront qu'un moyen de vote supplémentaire et facultatif.

II. Suffrage équitable

5. Dans toute élection ou référendum, un électeur ne pourra pas déposer plus d'un seul bulletin dans l'urne électronique. Un électeur ne sera autorisé à voter que s'il est établi que son bulletin n'a pas encore été déposé dans l'urne électronique.

6. Le système de vote électronique empêchera l'électeur d'exprimer son vote par plusieurs modes de suffrage.

7. Tout bulletin déposé dans une urne électronique sera comptabilisé, et tout suffrage exprimé lors d'une élection ou d'un référendum ne sera comptabilisé qu'une seule fois.

8. Lorsque des modes de vote électronique et non électronique sont utilisés dans un même scrutin, une méthode sûre et fiable permettra d'additionner tous les suffrages et de calculer le résultat correct.

III. Suffrage libre

9. L'organisation du vote électronique garantira la libre formation et expression de l'opinion de l'électeur, et, au besoin, l'exercice personnel du droit de vote.

10. La manière dont les électeurs sont guidés durant la procédure de vote électronique ne les amènera pas à voter dans la précipitation ou de manière irréfléchie.

11. Les électeurs pourront modifier leur choix à n'importe quelle étape de la procédure de vote électronique avant l'enregistrement de leur suffrage, ou même interrompre la procédure, sans que leur choix précédent ne soit enregistré ou que des tiers puissent en prendre connaissance.

12. Le système de vote électronique n'autorisera pas les influences destinées à manipuler la volonté de l'électeur pendant le vote.

13. Le système de vote électronique offrira à l'électeur un moyen de participer à une élection ou à un référendum sans qu'il ait à exprimer une préférence pour l'une quelconque des options de vote, par exemple en déposant un vote blanc.

14. Le système de vote électronique indiquera clairement à l'électeur que le suffrage a été enregistré avec succès et à quel moment la procédure de vote est terminée.

15. Le système de vote électronique rendra impossible toute modification d'un suffrage une fois qu'il aura été enregistré.

IV. Vote secret

16. Le vote électronique sera organisé de manière à préserver le secret du vote à toutes les étapes de la procédure, et en particulier lors de l'authentification de l'électeur.

17. Le système de vote électronique garantira que les suffrages exprimés dans l'urne électronique et le dépouillement sont et resteront anonymes, et qu'il est impossible d'établir un lien entre le vote et l'électeur.

18. Le système de vote électronique sera conçu de telle manière que le nombre de suffrages attendus dans une urne électronique ne permette pas d'établir un lien entre le résultat et les électeurs individuels.

19. Des mesures seront prises pour que les informations requises lors du traitement électronique ne puissent être utilisées pour violer le secret du vote.

B. Garanties de procédure

I. Transparence

20. Les Etats membres prendront des mesures afin que les électeurs comprennent le système de vote électronique utilisé et aient ainsi confiance en lui.

21. Des informations sur le fonctionnement du système de vote électronique seront diffusées auprès du public.

22. Les électeurs se verront offrir la possibilité de s'exercer sur tout nouveau système de vote électronique avant l'enregistrement du suffrage et indépendamment de celui-ci.

23. La possibilité sera offerte à tous les observateurs, dans les limites fixées par la loi, d'assister à l'élection électronique, de l'observer et de la commenter, y compris au stade de l'établissement des résultats.

II. Vérification et responsabilité

24. Les composants du système de vote électronique seront divulgués au moins aux autorités électorales compétentes, selon les besoins de la vérification et de l'homologation.

25. Avant la mise en service de tout système de vote électronique, et à intervalles réguliers par la suite, en particulier si des changements ont été apportés au système, un organisme indépendant désigné par les autorités électorales compétentes vérifiera que le système de vote électronique fonctionne correctement et que toutes les mesures de sécurité nécessaires ont été prises.

26. Le système offrira une possibilité de second dépouillement. D'autres caractéristiques du système de vote électronique qui pourraient peser sur l'exactitude du résultat seront vérifiables.

27. Le système de vote électronique n'empêchera pas la nouvelle tenue, partielle ou complète, d'une élection ou d'un référendum.

III. Fiabilité et sécurité

28. Les autorités des Etats membres garantiront la fiabilité et la sécurité du système de vote électronique.

29. Toutes les mesures possibles seront prises pour écarter les risques de fraude ou d'intervention non autorisée affectant le système pendant toute la procédure de vote.

30. Le système de vote électronique comportera des mesures visant à préserver la disponibilité de ses services durant la procédure de vote électronique. Il résistera en particulier aux dérangements, aux pannes et aux attaques en déni de service.

31. Avant toute élection ou référendum électronique, l'autorité électorale compétente vérifiera et établira elle-même que le système de vote électronique est authentique et fonctionne correctement.

32. Seules les personnes autorisées par l'autorité électorale auront accès à l'infrastructure centrale, aux serveurs et aux données relatives au vote. Ces autorisations seront soumises à des règles claires. Les interventions techniques sensibles seront réalisées par des équipes d'au moins deux personnes. La composition de ces équipes changera régulièrement. Dans la mesure du possible, de telles interventions seront réalisées en dehors des périodes électorales.

33. Durant la période d'ouverture d'une urne électronique, toute intervention autorisée affectant le système sera réalisée par des équipes d'au moins deux personnes, fera l'objet d'un compte rendu et sera contrôlée par des représentants de l'autorité électorale compétente et par tout observateur électoral.

34. Le système de vote électronique préservera la disponibilité et l'intégrité des suffrages. Il assurera également leur confidentialité et les gardera scellés jusqu'au moment du dépouillement. Si les suffrages sont stockés ou transmis hors des environnements contrôlés, ils seront cryptés.

35. Les votes et les informations relatives aux électeurs resteront scellés aussi longtemps que ces données seront conservées d'une manière qui permette d'établir le lien entre les deux. Les informations d'authentification seront sépa-

rées de la décision de l'électeur à une étape prédéfinie de l'élection électronique ou du référendum électronique.

Annexe II

Normes opérationnelles

I. Notification

36. Les règles internes régissant une élection ou un référendum électroniques établiront un calendrier clair de toutes les étapes du scrutin ou référendum, aussi bien avant qu'après celui-ci.

37. La période pendant laquelle un vote électronique pourra être enregistré ne commencera pas avant la notification du scrutin ou du référendum. En particulier pour ce qui est du vote électronique à distance, cette période sera définie et rendue publique bien avant le début du scrutin.

38. Bien avant le début du scrutin, les électeurs seront informés dans un langage clair et simple de la manière dont le vote électronique sera organisé et de toutes les démarches qu'ils pourraient avoir à effectuer pour y participer et voter.

II. Electeurs

39. Une liste électorale sera régulièrement mise à jour. L'électeur pourra au moins vérifier les données le concernant qui y figurent et demander des corrections.

40. La possibilité de créer une liste électorale électronique et un mécanisme permettant de s'y inscrire en ligne, et, le cas échéant, de demander à voter par voie électronique, sera envisagée. Si la participation au vote électronique nécessite une inscription séparée et/ou des démarches supplémentaires de la part de l'électeur, cela pourra se faire par voie électronique et une procédure interactive sera envisagée dans la mesure du possible.

41. Dans les cas où la période d'inscription des électeurs et les dates du scrutin coïncident, des dispositions adéquates seront prises pour l'authentification des électeurs.

III. Candidats

42. La déclaration de candidature en ligne pourra être envisagée.

43. Une liste de candidats produite et mise à disposition par voie électronique sera également accessible publiquement par d'autres moyens.

IV. Vote

44. Lorsque le vote électronique à distance se déroule pendant l'ouverture des bureaux de vote, il conviendra tout particulièrement de veiller à ce que le système soit conçu de manière à empêcher tout électeur de voter plusieurs fois.

45. Le vote électronique à distance pourra commencer et se terminer avant les heures d'ouverture de tout bureau de vote. Il ne se poursuivra pas après la clôture du scrutin dans les bureaux de vote.

46. Pour chaque mode de suffrage électronique, des modalités d'aide et d'assistance concernant les procédures de vote seront établies et mises à la disposition des électeurs. Pour le vote électronique à distance, ces modalités seront également accessibles par des moyens de communication différents et généralement accessibles.

47. Toutes les options de vote seront présentées de manière égale sur l'appareil utilisé pour l'enregistrement du vote électronique.

48. Le bulletin électronique servant à enregistrer le suffrage sera exempt de toute information sur les options de vote autre que ce qui est strictement nécessaire à l'expression du suffrage. Le système de vote électronique évitera l'affichage d'autres messages susceptibles d'influencer le choix de l'électeur.

49. S'il est décidé de permettre l'accès à des informations sur les options de vote à partir du site de vote électronique, ces informations seront présentées de manière égale.

50. L'attention des électeurs utilisant un système de vote électronique sera explicitement attirée sur le fait que l'élection ou le référendum électroniques pour lequel ils vont enregistrer leur vote par des moyens électroniques est une élection ou un référendum réel. S'il s'agit de tests, l'attention des participants sera explicitement attirée sur le fait qu'ils ne sont pas en train de participer à une élection ou un référendum réel, et ceux-ci seront – si les tests sont concomitants aux scrutins – dans le même temps invités à participer à ce scrutin par le(s) mode(s) de suffrage mis à leur disposition à cette fin.

51. Le système de vote électronique à distance ne permettra pas à l'électeur d'obtenir une preuve du contenu du suffrage qu'il a enregistré.

52. Dans un environnement supervisé, les informations relatives au suffrage disparaîtront de l'affichage vidéo, audio ou tactile utilisé par l'électeur pour exprimer son suffrage dès l'enregistrement de ce dernier. Quand une preuve papier du vote [électronique] est remise à l'électeur dans le bureau de vote, l'électeur ne doit pas avoir la possibilité de la montrer à toute autre personne ni d'emporter cette preuve à l'extérieur.

V. Résultats

53. Le système de vote électronique ne permettra pas de divulguer le nombre de suffrages exprimés pour les différentes options de vote avant la fermeture de l'urne électronique. Cette information ne sera révélée au public qu'après la clôture de la période du scrutin.

54. Le système de vote électronique empêchera que le traitement d'informations relatives aux suffrages exprimés relativement à des sous-ensembles de votants choisis délibérément puisse révéler les décisions individuelles des électeurs.

55. Tout décodage nécessaire au dépouillement des voix interviendra dès que possible après la clôture de la période du scrutin.

56. Les représentants de l'autorité électorale compétente pourront participer au dépouillement des votes, et les éventuels observateurs pourront observer leur comptabilisation.

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

58. En cas d'irrégularité entachant l'intégrité de certains suffrages, ceux-ci seront notés comme tels.

VI. Audit

59. Le système de vote électronique pourra faire l'objet d'un audit.

60. Les conclusions de l'audit seront prises en compte dans la préparation d'élections et de référendums ultérieurs.

Annexe III

Exigences techniques

La conception d'un système de vote électronique sera accompagnée d'une évaluation détaillée des risques qui peuvent compromettre le bon déroulement de l'élection ou du référendum concerné. Le système de vote électronique sera doté des garanties appropriées, fondées sur cette évaluation des risques, pour faire face aux risques identifiés. Les interruptions ou perturbations de service seront maintenues dans des limites prédéfinies.

A. Accessibilité

61. Des mesures seront prises pour garantir que les logiciels et les services concernés puissent être utilisés par tous les électeurs et, si nécessaire, pour fournir un accès à d'autres modes de vote.

62. Les utilisateurs seront impliqués dans la conception des systèmes de vote électronique, en particulier pour identifier les contraintes et tester la facilité d'utilisation à chaque étape majeure du processus d'élaboration.

63. Les utilisateurs se verront offrir, si la demande en est faite et que la possibilité existe, des fonctions complémentaires telles que des interfaces spéciales ou d'autres ressources équivalentes, comme une assistance personnelle. Les fonctions d'utilisateur seront, autant que possible, conformes aux directives de l'Initiative d'accès au Web (Web Accessibility Initiative-WAI).

64. Dans la conception de nouveaux produits, il conviendra de veiller à leur compatibilité avec les produits existants, y compris ceux utilisant des technologies d'assistance aux personnes handicapées.

65. La présentation des options de vote sera optimisée pour l'électeur.

B. Interopérabilité

66. Des normes ouvertes seront utilisées pour garantir l'interopérabilité des divers éléments techniques ou services d'origines éventuellement différentes d'un même système de vote électronique.

67. Actuellement, l'EML *(Election Markup Language)* est une telle norme ouverte et, afin de garantir l'interopérabilité, l'EML sera utilisée autant que possible dans les applications destinées aux élections et référendums électroniques. Le délai du passage des procédures de vote électronique actuelles à l'EML est laissé à l'appréciation des Etats membres. La norme EML en vigueur lors de l'adoption de cette recommandation et la documentation explicative sont disponibles sur le site du Conseil de l'Europe.

68. Les besoins spécifiques en matière de données électorales ou référendaires seront gérés par un processus d'adaptation aux conditions locales. Cela permettra d'étendre ou de restreindre les informations à fournir, tout en préservant leur compatibilité avec la version générique de l'EML. La procédure recommandée est l'utilisation d'un langage de schéma structuré et de modélisation.

C. Fonctionnement des systèmes
(pour l'infrastructure centrale et les clients dans des environnements contrôlés)

69. Les autorités électorales compétentes publieront une liste officielle des logiciels utilisés durant un vote ou référendum électronique. Les Etats membres peuvent, pour des raisons de sécurité, omettre les logiciels de sécurité de cette liste. Celle-ci spécifiera au minimum les logiciels utilisés, leur version et leur date d'installation, et fournira une brève description. Une procédure sera établie pour l'installation régulière des mises à jour et des corrections des logiciels de protection concernés. L'état de protection des équipements de vote pourra être vérifié à tout moment.

70. Les personnes en charge du fonctionnement des équipements définiront une procédure de secours. Tout système de remplacement répondra aux mêmes normes et exigences que le système original.

71. Des mesures de secours suffisantes seront mises en place et disponibles en permanence afin d'assurer un déroulement sans heurts du scrutin. Le personnel concerné sera prêt à intervenir rapidement selon une procédure établie par les autorités électorales compétentes.

72. Les responsables de l'équipement disposeront de procédures pour garantir que, durant le déroulement du scrutin, les équipements de vote et leur utilisation satisfont aux exigences requises. Des protocoles de contrôle seront régulièrement fournis aux services de secours.

73. Avant chaque scrutin ou référendum, l'équipement sera vérifié et approuvé conformément à un protocole établi par les autorités électorales compétentes. L'équipement sera vérifié afin de garantir sa conformité aux spécifications techniques. Les conclusions seront soumises aux autorités électorales compétentes.

74. Toute opération technique sera soumise à une procédure officielle de contrôle. Tout changement substantiel sur un équipement clé sera notifié.

75. Les équipements clés du vote ou référendum électronique seront situés dans une zone protégée, gardée en permanence contre des interférences de toutes sortes et de toute personne pendant la période du scrutin ou du référendum. Un plan de prévention des risques physiques sera mis en place pendant la période du scrutin ou du référendum. De plus, toutes les données conservées après la période du scrutin ou du référendum le seront en lieu sûr.

76. En cas d'incident susceptible d'affecter l'intégrité du système, les personnes chargées du fonctionnement de l'équipement en informeront immédiatement les autorités électorales compétentes, qui prendront les mesures nécessaires pour en atténuer les effets. Le niveau d'incident à signaler sera spécifié à l'avance par les autorités électorales.

D. Sécurité

I. Exigences générales
(concerne les périodes préélectorale, du scrutin et postélectorale)

77. Des mesures techniques et organisationnelles seront prises pour s'assurer qu'aucune donnée ne sera définitivement perdue en cas de panne ou de défaut affectant le système de vote électronique.

78. Le système de vote électronique préservera la vie privée des personnes. La confidentialité des listes électorales enregistrées ou communiquées par le système sera assurée.

79. Le système de vote électronique vérifiera régulièrement la conformité aux spécifications techniques du fonctionnement de ses éléments et la disponibilité de ses services.

80. Le système de vote électronique restreindra l'accès à ses services, en fonction de l'identité de l'utilisateur ou de son rôle, aux services explicitement ouverts à cet utilisateur ou à ce rôle. L'identité de l'utilisateur sera établie avant toute action.

81. Le système de vote électronique ou ses éléments protègeront les données d'authentification de manière à empêcher des entités non autorisées de détourner, d'intercepter, de modifier ou de prendre connaissance de toute autre manière de tout ou partie de ces données. Dans des environnements non contrôlés, il est recommandé de recourir à une authentification fondée sur la cryptographie.

82. L'identification des électeurs et des candidats sera assurée d'une manière qui permette de les distinguer sans le moindre doute de toute autre personne (identification exclusive).

83. Le système de vote générera des données d'observation assez détaillées et fiables pour permettre l'observation du scrutin. Il sera possible de déterminer de manière fiable la date et l'heure à laquelle un événement a généré des données d'observation. L'authenticité, la disponibilité et l'intégrité des données d'observation seront assurées.

84. Le système de vote électronique sera doté d'horloges synchronisées fiables. La précision de ce système d'horodatage sera suffisante pour gérer l'enregistrement de la date et l'heure des relevés d'audit et des données d'observation, ainsi que les limites des délais d'inscription, de désignation, de vote ou de dépouillement.

85. Les autorités électorales assumeront la responsabilité générale du respect de ces exigences de sécurité, qui seront contrôlées par des organismes indépendants.

II. Exigences en période préélectorale
(et pour les données transmises en période de scrutin)

86. 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.

87. Il sera possible d'établir si la désignation des candidats et, le cas échéant, la décision du candidat et/ou de l'autorité électorale compétente d'accepter une désignation sont intervenues dans les délais prescrits.

88. Il sera possible d'établir si l'inscription des électeurs est intervenue dans les délais prescrits.

III. Exigences pendant la période du scrutin
(et pour les données transmises à la période postélectorale)

89. L'intégrité des données communiquées à partir de la période préélectorale (par exemple les listes électorales et les listes des candidats) sera assurée. L'origine des données sera authentifiée.

90. On garantira que le système de vote électronique présente un bulletin authentique à l'électeur. En cas de vote électronique à distance, l'électeur sera informé des moyens de vérifier que la connexion est établie avec le serveur authentique et qu'un bulletin authentique lui est présenté.

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

92. Des mesures suffisantes seront prises pour assurer la protection des systèmes utilisés par les électeurs pour exprimer leur suffrage contre des influences pouvant modifier leur décision.

93. Les informations résiduelles qui renferment la décision de l'électeur ou l'image d'écran où s'affiche son choix seront détruites dès que le suffrage est exprimé. En cas de vote électronique à distance, l'électeur sera informé de la procédure à suivre pour effacer, si possible, les traces du suffrage exprimé de l'appareil utilisé pour enregistrer son suffrage.

94. Le système de vote électronique vérifiera en premier lieu que l'utilisateur qui essaie de voter est habilité à le faire. Le système authentifiera l'électeur et

s'assurera que seul le nombre approprié de suffrages par électeur sera enregistré et stocké dans l'urne électronique.

95. Le système de vote électronique garantira que la décision de l'électeur sera représentée avec exactitude dans le suffrage exprimé et que le vote scellé parviendra à l'urne électronique.

96. A l'issue de la période du scrutin électronique, aucun électeur n'aura accès au système de vote électronique. L'acceptation des suffrages électroniques dans l'urne électronique se poursuivra toutefois pendant un délai acceptable pour tenir compte des éventuels retards de transmission des messages au travers des différents modes de vote électronique.

IV. Exigences pendant la période postélectorale

97. L'intégrité des données communiquées pendant la période du scrutin (par exemple votes, inscription des électeurs, listes de candidats) sera préservée. L'origine des données sera authentifiée.

98. Le dépouillement décomptera les voix avec précision. Il sera reproductible.

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

E. Audit

I. Général

100. Le système d'audit sera conçu et implanté comme une partie intégrante du système de vote électronique. Des fonctions d'audit existeront à différents niveaux du système : logique, application et technique.

101. Un audit complet d'un système de vote électronique inclura l'enregistrement, la fourniture des fonctions de contrôle et celle des fonctions de vérification. C'est pourquoi des systèmes d'audit possédant les caractéristiques exposées aux sections II à V ci-dessous seront utilisés pour satisfaire à ces exigences.

II. Enregistrement

102. Le système d'audit sera ouvert et complet, et signalera activement les problèmes et menaces potentiels.

103. Le système d'audit enregistrera les dates et les heures, les événements et les actions, y compris :

a. toutes les informations relatives au scrutin, y compris le nombre d'électeurs habilités, le nombre de suffrages exprimés, le nombre de votes déclarés invalides, le dépouillement des votes, etc.;

b. toute attaque contre le système de vote électronique et ses infrastructures de communication ;

c. les pannes du système, ses défaillances et les autres menaces contre le système.

III. Contrôle

104. Un système d'audit permettra de surveiller l'élection ou le référendum et de vérifier la conformité des résultats et des procédures électorales aux dispositions légales pertinentes.

105. Les informations de l'audit ne seront pas divulguées à des personnes non autorisées.

106. Le système d'audit préservera constamment l'anonymat des électeurs.

IV. Vérification

107. Le système d'audit permettra de faire le contrôle croisé et la vérification du bon fonctionnement du système de vote électronique et de l'exactitude du résultat, de détecter les fraudes des électeurs et de fournir la preuve que tous les suffrages comptabilisés sont légitimes et que tous les votes authentiques sont comptabilisés.

108. Un audit permettra de vérifier qu'un scrutin ou un référendum électronique s'est déroulé conformément aux dispositions juridiques applicables, l'objectif étant d'établir que les résultats représentent les suffrages authentiques de manière exacte.

V. Divers

109. Le système d'audit sera protégé contre les attaques susceptibles de corrompre, d'altérer ou de détruire ses propres données.

110. Les Etats membres prendront les mesures nécessaires pour garantir la confidentialité de toute information obtenue par toute personne participant à l'audit.

F. Homologation

111. Les Etats membres sont invités à mettre en place des procédures d'homologation permettant de tester tout élément informatique et de vérifier sa conformité aux exigences techniques décrites dans cette recommandation.

112. Soucieux d'améliorer la coopération internationale et d'éviter les doubles emplois, les Etats membres envisageront de faire adhérer leurs organismes respectifs qui ne l'auraient pas encore fait aux accords internationaux pertinents de reconnaissance mutuelle tels que la Coopération européenne pour l'accréditation (European Co-operation for Accreditation-EA), la Coopération internationale sur l'agrément des laboratoires d'essais (International Laboratory Accreditation Cooperation-ILAC), le Forum international de l'accréditation (International Accreditation Forum-IAF) et les autres organismes similaires.

Exposé des motifs

Contexte

1. Des normes communes sur le vote électronique, fondées sur les principes des élections et référendums démocratiques et les appliquant aux aspects spécifiques du vote électronique, sont une condition essentielle en vue de garantir le respect de l'ensemble des principes des élections et référendums démocratiques dans le cadre du vote électronique, et d'établir ainsi la crédibilité des systèmes nationaux de vote électronique.

2. L'existence de normes communes est également un facteur déterminant l'interopérabilité des systèmes de vote électronique, condition de la mise au point de systèmes sûrs et efficaces. D'un point de vue strictement juridique et opérationnel, l'interopérabilité transfrontalière des systèmes de vote électronique en Europe ne semble pas être une nécessité ; lors de l'adoption de la recommandation, il n'existait aucune procédure électorale transfrontalière en Europe, hormis certaines procédures d'échange de données concernant un petit groupe d'électeurs au sein de l'électorat du Parlement européen. Néanmoins, le respect de normes techniques ouvertes et l'interopérabilité des systèmes à l'intérieur d'un pays et par-delà les frontières permettent d'utiliser parallèlement ou successivement des systèmes de vote électronique provenant de fournisseurs différents tout en réduisant leur coût d'achat pour les autorités nationales.

3. Les normes relatives au vote électronique sont un ensemble de normes juridiques et opérationnelles (aspects liés à l'organisation et aux procédures principalement) ainsi que de normes techniques fondamentales. Les normes juridiques ont pour objet d'appliquer les principes des instruments du Conseil de l'Europe et d'autres instruments internationaux en vigueur, en matière de vote, au contexte du vote électronique.

4. La recommandation a été établie par le Groupe ad hoc multidisciplinaire de spécialistes sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (IP1-S-EE). Ce groupe intergouvernemental composé de représentants de tous les Etats membres a été fondé par le Comité des Ministres et est chargé d'élaborer un ensemble de normes relatives au vote électronique, qui tienne compte des différentes conditions dans les Etats membres du Conseil de l'Europe, afin qu'elles soient appliquées par l'industrie informatique.

Champ de la recommandation

5. La recommandation comprend les élections et les référendums politiques, qui appartiennent tous deux au patrimoine démocratique européen ; l'application de normes se justifie dans un cas comme dans l'autre. Elections et référendums peuvent avoir lieu à différents niveaux. Certains pays ne tiennent pas de référendums ; dans d'autres, les niveaux mentionnés dans la recommandation ne sont pas tous concernés.

Raisons d'introduire ou d'envisager d'introduire le vote électronique

6. Les raisons d'introduire ou d'envisager d'introduire le vote électronique à un ou plusieurs niveaux d'une élection ou d'un référendum politique peuvent varier d'un pays à l'autre. Elles dépendent du contexte national propre à chaque pays.

Souveraineté des Etats membres en matière électorale

7. La souveraineté des Etats membres du Conseil de l'Europe en matière d'élections et de référendums n'est pas touchée par la présente recommandation. Les références à l'Union européenne visent à inclure les élections au Parlement européen dans le champ de la recommandation.

Principes régissant les élections et les référendums démocratiques

8. On ne peut concevoir la démocratie sans élection ou référendum organisé(e) dans le respect de certains principes qui leur confèrent un caractère démocratique. En 2002, la Commission européenne pour la démocratie par le droit (Commission de Venise) a adopté un Code de

bonne conduite en matière électorale[1]; il s'agit d'un instrument non contraignant qui définit cinq principes fondamentaux : le suffrage doit être universel, égal, libre, secret et direct. Ces cinq principes font partie du patrimoine démocratique de l'Europe[2] et s'appliquent tout autant aux élections et référendums qu'ils soient électroniques ou non.

9. Bien qu'il n'existe pas de définition généralement reconnue de ces principes, leur signification peut, aux fins du présent exposé des motifs, être résumée comme suit :

– *suffrage universel* : tout individu a le droit de vote et d'éligibilité, sous réserve de certaines conditions, telles que son âge et sa nationalité ;

– *suffrage égal* : chaque électeur a le même nombre de voix ;

– *suffrage libre* : l'électeur a le droit de former et d'exprimer librement son opinion, sans être soumis à une contrainte ou à une influence excessive ;

– *vote secret*: l'électeur a le droit de voter dans le secret, à titre individuel, et l'Etat a le devoir de protéger ce droit ;

– *suffrage direct* : les suffrages des électeurs déterminent directement la (les) personne(s) élue(s).

---

1. Code de bonne conduite en matière électorale (Commission de Venise – Opinion 190/2002_el), approuvé par la Résolution 1320 (2003) de l'Assemblée parlementaire et la Résolution 148 du CPLRE (2003), Déclaration du Comité des Ministres (114e session, 13 mai 2004).

2. – Le point 7 du document de la réunion de Copenhague de la Conférence sur la dimension humaine de l'OSCE du 29 juin 1990 fait explicitement référence au suffrage libre, universel, égal et secret ; le point 6 mentionne le suffrage direct, quoique sous une forme nuancée.

– L'article 25.*b* du Pacte international relatif aux droits civils et politiques prévoit expressément tous ces principes, sauf celui du suffrage direct, qui n'est énoncé qu'implicitement (article 21 de la Déclaration universelle des droits de l'homme).

– L'article 3 du Protocole additionnel à la Convention européenne des Droits de l'Homme prévoit explicitement le droit à des élections libres au scrutin secret, tenues à des intervalles raisonnables ; les autres principes ont, eux aussi, été reconnus dans la jurisprudence en matière de droits de l'homme (universalité : CEDH n° 9267/81, arrêt dans l'affaire Mathieu-Mohin et Clerfayt contre la Belgique, 2 mars 1997, Série A vol. 113, p. 23 ; arrêt dans l'affaire Gitonas et autres contre la Grèce, 1er juillet 1997, n° 18747/91, 19376/92 ; 19379/92, 28208/95 et 27755/95, *Recueil des arrêts et décisions*, 1997-IV, p. 1233 ; concernant l'égalité : arrêt précité dans l'affaire Mathieu-Mohin et Clerfayt, p. 23.). Le droit à des élections au suffrage direct a été implicitement admis par la Cour de Strasbourg (CEDH n° 24833/ 94, arrêt dans l'affaire Matthews contre le Royaume-Uni, 18 février 1999, *Recueil des arrêts et décisions*, 1999-I, paragraphe 64.)

10. Bien que ces principes soient généralement admis, leur mise en œuvre dans le contexte du vote électronique soulève un certain nombre de questions, qui nécessitent un examen approfondi. Toutefois, compte tenu des spécificités du vote électronique, ces questions ne revêtent pas la même importance selon qu'on considère tel ou tel des cinq principes. Alors que les principes du suffrage universel, égal, libre et secret exigent que des dispositions particulières soient prises dans le contexte du vote électronique, cela n'est pas le cas du principe du suffrage direct – lequel, en conséquence, n'est pas traité dans la recommandation.

11. Les normes énoncées dans la recommandation traitent exclusivement de questions concernant spécifiquement le vote électronique. Les principes généraux des élections et référendums démocratiques ne sont pas réitérés.

Normes juridiques, opérationnelles et techniques

12. Les annexes I à III de la recommandation comportent un ensemble de normes juridiques, opérationnelles et techniques. Il s'agit de normes minimales dont l'application aux systèmes de vote électronique peut aider à en assurer la conformité aux principes des élections et des référendums démocratiques, sans toutefois constituer à elle seule une garantie de qualité démocratique. L'évaluation d'un vote électronique doit se fonder sur un examen approfondi de la procédure dans son ensemble, en tenant compte de son contexte. A cet égard, le respect des normes est un élément important qui aide à assurer la qualité démocratique du système de vote électronique.

13. Les trois catégories de normes sont étroitement liées. Il convient d'en tenir compte lors de la mise en œuvre de la recommandation :

– les normes juridiques ont trait au contexte juridique dans lequel le vote électronique est valable ;

– les normes opérationnelles ont trait au mode d'utilisation et d'entretien des logiciels et du matériel employés dans le cadre du vote électronique ;

– les normes techniques ont trait au développement et au fonctionnement des logiciels et du matériel employés dans le cadre du vote électronique. L'adoption des normes techniques permet d'assurer la

sécurité technique, l'accessibilité et l'interopérabilité des systèmes de vote électronique.

Les trois catégories de normes incluent des dispositions relatives à toutes les étapes de la consultation (étapes préélectorale, du scrutin, et post-électorale). L'interconnexion peut concerner, selon le cas, les trois étapes, ou seulement une ou deux d'entre elles.

i. Déclaration introductive («Le vote électronique doit respecter…»)

14. Cette déclaration introductive traite de plusieurs questions qui ont une importance générale dans le contexte des élections et référendums électroniques.

15. Les systèmes de vote non électronique existants ont été conçus en veillant au respect des principes du vote démocratique. Lors de l'introduction de nouveaux modes de suffrage, il est essentiel de ne pas porter atteinte à ces principes ; en conséquence, les systèmes de vote électronique doivent être conçus et utilisés de manière à garantir la fiabilité et la sécurité du processus de vote à l'égal des systèmes de vote non électronique dans l'Etat concerné.

16. Pour garantir qu'un système de vote électronique produise des élections ou référendums conformes aux principes généraux, il peut être nécessaire d'attacher davantage d'importance à l'application de tel principe plutôt que de tel autre. Toutefois, le résultat doit toujours être le respect des principes dans leur ensemble.

17. La comparaison avec le système de vote non électronique dans l'Etat concerné ne signifie pas que le vote électronique doit être aussi sûr et fiable que l'ensemble des modes de suffrage non électronique. Le principe qui sous-tend la recommandation est qu'un système de vote électronique à distance doit être – globalement – aussi sûr qu'un système de vote à distance non électronique sans surveillance ; de même, un système de vote électronique local doit être aussi sûr qu'un système de vote local non électronique.

18. D'autre part, la comparaison avec les systèmes de vote non électronique ne devrait pas empêcher un Etat de modifier son système de vote non électronique tant que les changements sont conformes à tous les principes des élections et référendums démocratiques.

19. La comparaison des niveaux de fiabilité, de sécurité ou autres lors de la mise en place du vote électronique ne vise pas à rendre immuables les niveaux atteints respectivement par les modes de suffrage non électronique, notamment lorsqu'il est possible et nécessaire d'améliorer la mise en œuvre des principes du vote démocratique.

ii. Examen de la législation interne

20. Il est dit, dans la recommandation, que les Etats membres devraient étudier la possibilité de revoir leur législation pertinente quand ils optent pour le vote électronique. Il convient de prendre sérieusement en considération des aspects de la législation autres que ceux qui se rapportent simplement au matériel électronique nécessaire et à son utilisation. Quelle devrait être l'ampleur de l'examen en question ? Cela dépendra des lois de l'Etat membre concerné ; nous ne pouvons en donner ici une présentation exhaustive. Ce sont par exemple les lois pénales en matière électorale et celles relatives à la protection des données et à l'observation des élections.

iii. Adaptation aux circonstances locales

21. La présente recommandation a pour objet de proposer des normes communes pour le vote électronique. Dans certains Etats, l'organisation d'une élection ou d'un référendum suppose le respect de procédures très spécifiques de la part des pays concernés. Quand ces procédures spécifiques ne concernent qu'un tout petit nombre d'Etats membres, voire un seul, elles sont considérées comme des « particularités locales » et ne sont donc pas prises en compte dans la recommandation, mais sont toutefois évoquées dans l'exposé des motifs. Les pays concernés peuvent conserver leurs particularités locales et, s'ils le désirent, les adapter à l'avenir. Ils ne sont pas tenus de les abandonner ou de les modifier pour se conformer à la recommandation dans la mesure où ces particularités locales respectent les principes des élections et référendums démocratiques, et tous les engagements et obligations souscrits par les Etats membres.

iv. Durabilité

22. Le vote électronique est un nouveau domaine politico-technologique qui se développe rapidement. Il est nécessaire que les normes et

les exigences évoluent en fonction des nouveaux développements et, si possible, qu'elles les anticipent. C'est pourquoi le paragraphe v recommande que chaque Etat membre suive de près sa propre position sur le vote électronique et rende compte au Conseil de l'Europe des résultats des études qu'il a éventuellement réalisées. Le Conseil pourra examiner à nouveau cette question deux ans après l'adoption de la présente recommandation ; les Etats membres pourront avoir cette échéance à l'esprit lorsqu'ils apprécieront l'opportunité de procéder à une étude et, le cas échéant, lorsqu'ils en arrêteront la date, compte tenu de leur situation individuelle.

23. Dans le cadre du suivi, une révision de la recommandation pourra être envisagée dès que les Etats membres auront acquis davantage d'expérience en matière d'élections ou de référendums électroniques.

24. Les développements technologiques, imprévisibles au moment de l'adoption de la recommandation, ne peuvent permettre d'exclure l'éventualité selon laquelle un système quelconque – y compris l'*Election Markup Language* (EML) –, viable aujourd'hui, peut, un jour, ne plus être le système le plus approprié pour les élections ou les référendums électroniques et peut, ainsi, cesser d'être recommandé par un pays ou un groupe de pays.

Interprétation

25. Le paragraphe sur l'interprétation comporte les définitions des termes utilisés dans les différentes parties de la recommandation et de ses annexes. Il convient de tenir compte de ces définitions lors de la traduction de tout ou partie de la recommandation dans d'autres langues. L'annexe III comporte un glossaire technique de définitions des termes utilisés dans cette annexe.

Définition du vote électronique à distance

26. Le vote électronique peut s'effectuer à distance ou en local. De nombreux systèmes électoraux conjuguent le vote à distance et le vote local. Le vote à distance peut s'effectuer dans un environnement surveillé (ambassade, consulat, bureau de poste, mairie, etc.) ou non surveillé, c'est-à-dire en l'absence de représentants des services électoraux (vote par correspondance). Chaque Etat membre possède ses propres

pratiques établies en ce qui concerne les formes de vote offertes aux électeurs[1]. Pour les besoins de la recommandation, la distinction entre vote local et vote à distance ne suit pas les mêmes critères selon qu'il s'agit de vote traditionnel ou de vote électronique. Le vote électronique à distance désigne exclusivement une forme de vote électronique dans laquelle le vote se fait au moyen de dispositifs qui ne sont pas surveillés par des membres des services électoraux.

Annexe I

Normes juridiques

A. Principes

I. Suffrage universel

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

27. Aucun système de vote ne peut être compris et utilisé par tous les électeurs sans exception ; un système qui s'appuie sur des explications exclusivement visuelles, par exemple, ne peut être utilisé par les aveugles. Pour tenir des élections et des référendums démocratiques, les Etats membres doivent s'efforcer de faire en sorte que l'interface électeur d'un système de vote électronique soit utilisable et compréhensible par le plus de personnes possible.

Norme n° 2. «Les éventuelles procédures d'inscription au vote électronique...»

28. Cette disposition a pour but de garantir qu'aucun électeur ne soit empêché d'utiliser le vote électronique du fait de procédures d'inscription difficiles.

Norme n° 3. «Les systèmes de vote électronique seront conçus...»

29. L'accessibilité des systèmes de vote électronique doit être assurée dans toute la mesure du possible ; ceux-ci doivent être utilisés parallèlement à d'autres modes de suffrage de manière à ce que, toutes méthodes confondues, le plus

1. La Commission européenne pour la démocratie par le droit (Commission de Venise) a émis un avis sur la question du vote à distance et sa compatibilité avec les instruments du Conseil de l'Europe (adopté par la Commission de Venise lors de sa 58e session plénière, Venise, 12-13 mars 2004, Etude n° 260, 2003, Strasbourg, 18 mars 2004, CDL-AD (2004)012 Or. fr.). Dans ses conclusions, elle estime que le vote par correspondance et le vote électronique à distance sont compatibles avec les normes du Conseil de l'Europe sous réserve que les procédures employées comportent certains mécanismes préventifs.

grand nombre possible d'électeurs aient accès au vote. Certaines personnes handicapées ne sont pas en mesure d'utiliser le vote électronique. La conception des systèmes de vote électronique devrait viser à en exploiter toutes les possibilités d'accessibilité pour les personnes handicapées.

Norme n° 4. «A moins que les modes de vote électronique à distance ne soient...»

30. La mise en place de modes de vote électronique s'ajoutant aux modes de vote traditionnel peut rendre les élections plus accessibles et renforcer ainsi le principe d'universalité. En revanche, l'utilisation du vote électronique à distance à l'exclusion d'autres méthodes restreint l'accessibilité du vote. Cette disposition vise à protéger l'électeur de situations où les seuls modes de vote offerts ne lui seraient pas effectivement accessibles.

31. En ce qui concerne le vote électronique local, il convient de laisser aux Etats membres le soin de décider s'ils veulent offrir d'autres possibilités de voter. Cela correspond à la situation existante. Cependant, comme pour tout mode de suffrage local, les lieux de vote doivent être conformes aux normes d'accessibilité.

II. Suffrage équitable

Normes nos 5 et 6. «Un électeur ne pourra pas déposer...»

32. Le système de vote doit être conçu dans son ensemble de manière à ce qu'un électeur ne puisse voter plus d'une fois. Ce principe n'empêche pas que certains systèmes de vote permettent aux électeurs de choisir plus d'une option ; c'est le cas des systèmes de vote de préférence ou des scrutins doubles, comportant un volet national et un volet régional. La notion de suffrages multiples évoque le danger de voir enregistrer davantage de suffrages que ceux auxquels un électeur donné a droit. Cela peut arriver quand 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 au nom de celui-ci alors que cette personne a déjà voté en son nom propre.

33. Dans certains Etats membres, le système électoral prévoit la possibilité pour les électeurs de voter plus d'une fois, mais ne tient compte que du dernier vote. C'est notamment le cas dans les exemples suivants :

a. Au Danemark et en Suède, les systèmes de vote permettent aux électeurs de voter à l'avance et de modifier leur choix ultérieurement. Au Danemark, il est permis de voter à l'avance plusieurs fois. En Suède, le vote

à l'avance n'est autorisé qu'une seule fois. Dans les deux systèmes, seul le dernier vote est déposé dans l'urne et prend ainsi valeur de suffrage.

b. Au Royaume-Uni, si une personne se rend dans un bureau de vote pour voter et constate 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 de la validité de l'élection. Des dispositions analogues s'appliquent lorsque les services électoraux reçoivent deux votes par correspondance pour un seul et même électeur.

Norme n° 7. «Tout bulletin déposé...»

34. Il importe de compter l'ensemble des votes, qu'ils soient déposés par voie électronique ou traditionnelle.

III. Suffrage libre

Norme n° 9. «L'organisation du vote électronique...»

35. Le suffrage personnel, c'est-à-dire l'exercice personnel du droit de voter, est un principe fondamental dans nombre d'Etats membres. Etant donné sa grande vulnérabilité dans le contexte du vote électronique à distance, la recommandation lui porte une attention particulière. Cette norme ne constitue pas pour autant un obstacle au vote électronique à distance.

36. Certains Etats membres emploient des procédures de vote où, dans un souci d'accessibilité, le principe d'universalité prime sur le principe du suffrage personnel ; c'est pourquoi, par exemple, le vote par procuration y est autorisé.

37. Lorsque des moyens de vote électronique à distance sont mis à disposition, une attention particulière doit être accordée à la mise en place d'installations qui permettent à l'électeur d'exercer son droit d'exprimer un suffrage dans un environnement surveillé.

Norme n° 10. «La manière dont les électeurs...»

38. «De manière irréfléchie» signifie : sans avoir eu assez de temps pour y réfléchir.

Norme n° 11. «Les électeurs pourront modifier...»

39. Seul l'électeur doit avoir accès à son bulletin. Ainsi, les systèmes de vote électronique ne doivent pas enregistrer le bulletin rempli sur le dispositif de l'électeur en vue d'un dépôt ultérieur. Personne d'autre que l'électeur ne doit

avoir accès à son bulletin, ni sur le dispositif de vote, ni lors du transfert dans l'urne.

Norme n° 12. «Le système de vote électronique n'autorisera pas...»

40. Il convient d'exclure toute possibilité de manipulation, physique, électronique ou psychologique. Ainsi, les sons susceptibles d'être associés à un candidat ou à une option, les fenêtres avec des messages encourageant un choix donné et tout autre dispositif de ce genre sont à empêcher dans la mesure du possible.

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

41. Dans les systèmes de vote traditionnel, les électeurs ont la possibilité de voter blanc, c'est-à-dire de ne pas exprimer une préférence parmi les choix proposés. Cette norme établit que la possibilité de déposer un bulletin blanc doit être maintenue dans le contexte du vote électronique.

42. Il appartient à chaque Etat membre de déterminer si le système de vote électronique doit lui aussi permettre de déposer un bulletin de vote – rempli ou blanc – rendu intentionnellement nul.

Norme n° 14. «Le système de vote électronique indiquera clairement...»

43. En général, la procédure de vote est achevée avec succès lorsque le bulletin électronique est déposé dans l'urne électronique. Dans le contexte du vote électronique à distance, cela signifie que la procédure de vote n'est achevée qu'après que le bulletin est parvenu à destination, c'est-à-dire après son envoi depuis le dispositif de vote de l'électeur (ordinateur, téléphone, etc.), par Internet ou un autre réseau, au serveur faisant office d'urne électronique.

44. Le message confirme à l'électeur que son bulletin est déposé dans l'urne et qu'il sera donc compté. L'électeur sait alors qu'il a déposé son bulletin, aspect important du point de vue de la confiance apportée au système et compte tenu du principe selon lequel chaque bulletin déposé doit être pris en compte. En outre, l'électeur doit savoir à quel moment la procédure de vote est achevée afin de pouvoir interrompre la connexion sans dommage. Les deux messages (le dépôt du bulletin et l'achèvement de la procédure) peuvent être réunis en un seul si les deux moments coïncident.

IV. Vote secret

45. Tout système de vote électronique mis en place par un Etat donné doit être conforme aux obligations et engagements internationaux de cet Etat en matière de secret du vote.

Norme n° 16. «Le vote électronique sera organisé de manière à…»

46. Le principe du secret doit s'appliquer à la procédure tout entière, qui recouvre la période préélectorale (communication aux électeurs des numéros d'identification personnels, des codes candidats et des jetons électroniques), le remplissage et l'envoi du bulletin ainsi que le comptage et le recomptage des suffrages.

Norme n° 17. «Le système de vote électronique garantira que les suffrages…»

47. Cette norme énonce qu'il ne doit en aucun cas être possible d'établir un lien entre le contenu d'un bulletin déposé et un électeur.

48. Dans le contexte du vote électronique (à distance), une attention particulière doit être portée au principe du suffrage libre et secret. Seuls les électeurs autorisés à voter ont le droit de déposer un bulletin ; en conséquence, il convient d'identifier chaque électeur et de vérifier son droit de voter. L'étendue du processus d'identification (indication du nom de l'électeur, présentation d'une carte d'identité, etc.) varie selon les législations nationales, mais le principe de base est identique : pour éviter les votes multiples et autres abus, on identifie l'électeur et on vérifie s'il a déjà voté.

49. Il peut arriver que, à une certaine étape de la procédure de vote à distance, l'identité et le bulletin de l'électeur soient liés d'une quelconque manière. Si le contenu du bulletin était divulgué à cet instant, ou si le lien entre l'électeur et le bulletin était maintenu et le contenu du bulletin divulgué ultérieurement, le secret du vote serait violé. Dans les systèmes de vote traditionnel, la séparation entre l'identification de l'électeur et le bulletin est assurée au moyen d'une séparation physique. Celle-ci peut être aisément contrôlée par les membres des services électoraux et les observateurs. Dans les systèmes de vote électronique local, l'identification de l'électeur et le bulletin peuvent également être séparés physiquement, comme c'est le cas lorsque le dispositif de vote électronique n'est utilisé que pour le dépôt du bulletin. S'agissant des systèmes de vote électronique à distance, cette séparation doit être assurée par voie électronique. La séparation électronique nécessite des solutions techniques spécifiques. Il convient d'en tenir compte lors de l'introduction du vote électronique.

50. Dans les systèmes électoraux qui autorisent les électeurs à déposer un bulletin à l'avance et à le modifier ultérieurement (comme en Suède), il doit être possible d'identifier le bulletin scellé d'un électeur précis afin de pouvoir l'annuler. L'identification et l'annulation du bulletin doivent se faire sans compromettre le secret du vote ; en conséquence, le bulletin doit être totalement scellé tout au long des processus de vote, de conservation et d'annulation. Néanmoins, le bulletin scellé doit toujours être lié à un électeur précis.

51. La séparation entre le bulletin et l'identité de l'électeur doit se faire au plus tard au moment du dépôt du bulletin dans l'urne électronique, et ne doit en aucun cas être réversible.

52. Dans certains pays (comme au Royaume-Uni), la loi exige l'établissement d'un lien entre l'électeur et le bulletin, et son maintien pour une certaine durée au-delà de la date des élections. Il convient alors de veiller à ce que le lien entre l'électeur et son bulletin soit suffisamment protégé, durant toute la période concernée, pour garantir le secret du vote. Le secret ne peut être levé que sur décision d'une juridiction compétente, en veillant à ce qu'aucun électeur ne soit contraint de révéler comment il a voté.

Norme n° 19. «Des mesures seront prises pour que les informations requises...»

53. Entre autres mesures indispensables, il y a lieu, par exemple, de prévoir que les bulletins seront conservés dans un ordre aléatoire dans l'urne électronique. L'ordre dans lequel ils sont stockés ne doit pas permettre de déterminer l'ordre dans lequel ils sont arrivés.

B. Garanties de procédure

54. Les garanties de procédure permettent de s'assurer que tous les principes du vote démocratique sont appliqués et préservés dans le contexte du vote électronique.

I. Transparence

Norme n° 20. «Les Etats membres prendront des mesures afin que...»

55. La confiance que les systèmes de vote inspirent aux électeurs et aux candidats influence de manière déterminante le niveau de participation aux élections; c'est aussi un élément essentiel du système démocratique de l'Etat. La confiance a pour base une connaissance approfondie du système.

56. Les modes de suffrage traditionnel sont simples et ont largement fait leurs preuves dans les Etats membres. Les électeurs connaissent bien les systèmes électoraux utilisant des bulletins et des urnes, et comprennent les règles générales qui régissent la procédure à suivre par l'électeur ainsi que la collecte et le décompte des suffrages. L'introduction du vote électronique crée une nouvelle situation dans laquelle les électeurs sont moins au fait du processus électoral et peut-être moins en mesure de comprendre les dispositifs de sécurité que comporte le système. En conséquence, l'introduction des systèmes de vote électronique devra probablement s'accompagner de campagnes de communication afin de maintenir le niveau de connaissance et de confiance du public. A terme,

il pourra être nécessaire de poursuivre ces activités à l'intention des électeurs qui ne connaissent pas le vote électronique.

57. Pour accroître la confiance des électeurs, il convient de les informer le plus amplement possible sur les techniques employées dans le cadre du vote électronique.

Norme n° 22. «Les électeurs se verront offrir la possibilité de s'exercer...»

58. Un nouveau système de vote électronique peut générer des inquiétudes diverses chez les électeurs. Afin d'accroître le niveau d'information et de confiance des électeurs à l'égard des nouveaux systèmes de vote électronique, et dans un souci de transparence, il convient de leur donner la possibilité de s'exercer à l'utilisation de ces systèmes, avant un vote et indépendamment de celui-ci. Les catégories d'électeurs qui ne connaissent pas encore les nouveaux modes de suffrage électronique, par exemple les personnes âgées, doivent bénéficier à cet égard d'une attention particulière.

Norme n° 23. «…tous les observateurs, dans les limites fixées par la loi...»

59. Il existe diverses obligations internationales et nationales en matière d'observation d'élections : par des représentants des candidats, ainsi que par des observateurs indépendants – nationaux et/ou internationaux. Tous les Etats membres sont liés par le document de la réunion de Copenhague de la Conférence sur la dimension humaine de l'OSCE du 29 juin 1990, document dans lequel ils s'engagent à «inviter des observateurs de tout autre Etat participant à l'OSCE et de toute institution ou organisation privée compétente qui le souhaiterait, à suivre le déroulement de la procédure de leurs élections nationales [et] à faciliter un accès analogue pour les élections organisées à un niveau inférieur au niveau national».

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

61. Les élections et référendums électroniques sont porteurs de problèmes spécifiques, inhérents au déroulement électronique de la consultation. Ainsi, il faut que les observateurs aient la possibilité, notamment, d'accéder aux informations pertinentes relatives au logiciel ; il faut qu'ils puissent voir les mesures de sécurité physiques et électroniques pour les serveurs ; qu'ils puissent inspecter et tester les dispositifs homologués, avoir accès aux sites et aux informations

concernant le vote électronique à distance et procéder aux tests appropriés ; enfin, observer le dépôt des bulletins électroniques dans l'urne électronique, ainsi que le dépouillement. Toutefois, il peut s'avérer nécessaire, compte tenu des mesures de sécurité applicables aux liaisons téléphoniques ou par l'Internet, de ne pas autoriser la présence d'observateurs dans la salle des ordinateurs. Dans ce cas, il convient de prendre des mesures afin de donner aux observateurs la possibilité de contrôler les opérations.

II. Vérification et responsabilité

Norme n° 24. « Les composants du système de vote électronique… »

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

Norme n° 26. « Le système offrira une possibilité de second dépouillement. »

63. Le recomptage est une procédure visant à vérifier les résultats de la consultation électorale ou référendaire qui ont déjà été constatés. En matière de vote électronique, il existe différents moyens de procéder à un recomptage ; ces moyens diffèrent par leur complexité et par leur capacité à renforcer la fiabilité. Une méthode très simple de recomptage consiste à demander au système de vote électronique de procéder à un second décompte. On peut également transférer l'urne électronique dans un système de vote électronique analogue, mais distinct, et procéder au second décompte sur ce système. Une troisième possibilité consiste à recompter les suffrages au moyen d'un système de vote électronique différent du premier, mais compatible avec lui. Une quatrième option consiste à éditer des bulletins papier à une certaine étape de la procédure de vote et à les utiliser pour le recomptage.

64. Aux fins de la vérification des résultats, il n'est pas toujours suffisant de procéder au recomptage. Selon la configuration du système utilisé, il existe parfois d'autres éléments qui contribuent à l'exactitude du résultat. On peut mentionner, à titre d'exemple, la confirmation du fait que tous les suffrages exprimés ont bien été pris en compte.

Norme n° 27. «Le système de vote électronique n'empêchera pas…»

65. S'il devient nécessaire de tenir un nouveau scrutin dans le cadre d'un vote électronique, il est possible que ce nouveau scrutin ne puisse être tenu sans s'appuyer au moins partiellement sur le système de vote électronique utilisé lors du premier scrutin. Cela peut notamment être le cas lorsque l'identification des personnes autorisées à voter nécessite des informations accessibles à travers le système en question.

III. Fiabilité et sécurité

Norme n° 28. «Les autorités des Etats membres garantiront…»

66. Les nouveaux modes de suffrage doivent être aussi fiables et sûrs que les modes traditionnels ; et il appartient à l'Etat membre de s'en porter garant. La responsabilité finale ne peut en aucun cas être déléguée à un fournisseur de systèmes de vote.

Norme n° 29. «Toutes les mesures possibles seront prises…»

67. Avant de prendre une telle décision, on aura pesé l'importance respective de plusieurs facteurs. Par exemple, dans tel cas, on peut être amené à mettre en balance, d'une part, l'impératif sécuritaire – d'une importance capitale – et, d'autre part, la volonté de disposer d'un système qui soit facilement utilisable par les électeurs. En pareil cas, le souci de la convivialité ne doit pas l'emporter sur la nécessité de prévoir un haut niveau de sécurité ; cependant, cette commodité d'utilisation qu'on souhaite promouvoir peut constituer un élément dans le choix des mesures de sécurité à adopter. Un cas de figure analogue pourrait être celui dans lequel l'obtention d'un avantage supplémentaire minime en termes de sécurité impliquerait un coût disproportionné.

Norme n° 30. «Le système de vote électronique comportera des mesures…»

68. 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 (voir l'annexe III, norme n° 77).

Norme n° 31. «Avant toute élection ou référendum…»

69. Cette norme exige que le fonctionnement correct du système de vote électronique ait été vérifié (voir la norme n° 24). Il convient en outre de s'assurer que le système de vote électronique utilisé lors du scrutin est bien celui dont le fonctionnement a été vérifié. Cette disposition a pour but d'empêcher l'installation de systèmes de vote électronique ayant éventuellement fait l'objet de manipulations

ou de remplacements touchant l'ensemble du système ou certains de ses éléments. Les autorités compétentes doivent veiller à ce que les systèmes prévus soient utilisés.

Norme n° 33. «Durant la période d'ouverture d'une urne électronique...»

70. Le mot «tout» indique que, si la loi nationale permet la présence d'observateurs aux élections, l'accès doit leur être accordé. En ce qui concerne le vote par téléphone ou par l'Internet, il peut être nécessaire, par mesure de sécurité, de ne pas autoriser la présence d'observateurs dans la salle des ordinateurs. Dans ce cas, il convient de prendre des mesures afin de donner aux observateurs la possibilité de contrôler l'intervention.

Norme n° 34. «Le système de vote électronique préservera...»

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

72. Le scellement d'une urne requiert des mesures physiques et organisationnelles. Celles-ci peuvent inclure le verrouillage physique de l'urne et sa surveillance par plus d'une personne. En présence d'une urne électronique, des mesures complémentaires peuvent être nécessaires, telles que des contrôles d'accès, des structures d'autorisation et des murs pare-feu.

73. Le scellement d'un bulletin électronique en vue de sa transmission depuis le dispositif de l'électeur jusqu'à l'urne (située à distance) nécessite, outre des mesures physiques et organisationnelles, des mesures de cryptage.

74. Un bulletin est scellé lorsque son contenu a été soumis à des mesures faisant en sorte qu'il ne puisse être ni lu, ni modifié, ni relié à l'électeur qui l'a émis.

Annexe II

Normes opérationnelles

I. Notification

Norme n° 36. «Les règles nationales régissant...»

75. Les procédures à suivre par les électeurs peuvent varier selon qu'il s'agit d'un mode de suffrage traditionnel ou électronique. Les différences portent par

exemple sur la période pendant laquelle les votes peuvent être émis, la démarche que doit suivre l'électeur et le déroulement concret du vote. Elles devraient être communiquées aux électeurs afin de leur donner tous les éléments requis en vue de prendre une décision éclairée sur le choix du mode de suffrage, et afin d'éviter tout malentendu concernant la procédure de vote. Il convient de réfléchir au laps de temps nécessaire aux électeurs pour faire leur choix afin de déterminer la période la plus propice à cette campagne de communication.

Norme n° 37. «La période pendant laquelle un vote électronique pourra...»

76. La communication concernant la période pendant laquelle un vote peut être émis est particulièrement importante lorsque cette période varie selon le mode de suffrage. Cet aspect concerne plus particulièrement le vote à distance où, en raison des caractéristiques du vote électronique à distance, il peut être préférable d'instaurer des périodes de vote différentes pour le vote traditionnel et le vote électronique.

Norme n° 38. «Bien avant le début du scrutin, les électeurs...»

77. Il importe de décrire les procédures et les démarches devant être accomplies pour voter au moyen des modes de suffrage électronique, car ceux-ci impliquent généralement que l'utilisateur dispose de certains équipements. Le vote par l'Internet, par exemple, pourra être pratiqué par la plupart des personnes disposant d'un ordinateur capable de se connecter à l'Internet; il n'est cependant pas exclu qu'un faible pourcentage de machines ou de logiciels trop anciens ne permettent pas une telle utilisation. Il faut donc indiquer clairement le matériel nécessaire pour utiliser une méthode donnée. On envisagera également de donner aux utilisateurs la possibilité de vérifier la compatibilité de leur matériel avant de choisir un mode de suffrage. De même, les électeurs pourraient être autorisés à revenir sur leur choix d'un mode de suffrage électronique au cas où ils ne seraient pas en mesure d'utiliser le mode choisi. Un électeur pourrait ainsi passer du vote par l'Internet au vote par téléphone dans les cas où ces deux modes sont proposés.

II. Electeurs

Norme n° 39. «Une liste électorale...»

78. Il est nécessaire de vérifier, pour chaque votant, s'il a le droit de voter et s'il n'a pas déjà voté. Dans un contexte non électronique, il existe plusieurs moyens de procéder à ces vérifications. Ces vérifications peuvent prendre diverses formes qui vont de l'inscription matérielle dans un registre des électeurs qui ont

voté, à l'enregistrement électronique du fait qu'une personne a effectivement enregistré son suffrage.

79. Pour que ces vérifications soient précises, il est nécessaire que les listes en question contiennent des informations à jour indiquant qui a le droit de vote lors du scrutin ou du référendum en question. Il faut donc que ces listes soient actualisées avant la date de la consultation. Il convient de remarquer que l'utilisation du mot «liste» au singulier n'implique pas nécessairement l'existence d'une seule liste contenant les noms de tous les électeurs d'un pays ou d'une région.

80. Dans le cas du vote électronique à distance, ces vérifications donnent nécessairement lieu à l'utilisation de listes. Bien qu'il soit concevable que, dans certains cas, on puisse utiliser des listes papier, la plupart des systèmes de vote électronique à distance devront utiliser des listes électroniques. Lorsqu'un électeur a la possibilité d'utiliser un moyen de vote électronique à distance et, parallèlement, de voter dans un bureau de vote, les membres du service électoral de ce bureau doivent avoir la possibilité de vérifier si cet électeur a déjà, ou non, déposé son bulletin.

81. Dans la pratique, différentes procédures seront employées pour créer les listes en question. Certains pays possèdent des registres d'état civil qui recensent la quasi-totalité des électeurs (hormis, par exemple, les expatriés). Sur la base de ces registres, on peut obtenir, souvent à l'aide de procédures informatisées, la liste des personnes autorisées à voter (ou liste électorale). Dans les pays qui ne disposent pas de tels registres d'état civil, les listes électorales sont établies au moyen d'une procédure d'inscription dans laquelle, entre autres, il appartient aux électeurs de demander l'inscription. Ces procédures diffèrent d'un pays à l'autre.

82. Les électeurs devraient avoir la possibilité de vérifier s'ils sont correctement inscrits. Dans certains Etats membres, les listes électorales peuvent être rendues publiques (ou accessibles au public) ; dans d'autres, en vertu de la réglementation relative à la protection des données personnelles, chaque électeur ne peut vérifier que sa propre inscription.

Norme n° 40. «La possibilité de créer une liste électorale électronique…»

83. On peut concevoir des systèmes offrant aux électeurs la possibilité de s'inscrire en ligne. Cela suppose l'existence de listes électroniques et de dispositifs d'authentification électronique tels que les systèmes de signature numérique. Il est également possible de permettre aux électeurs de demander, en utilisant un dispositif électronique ou en ligne, à utiliser un mode de suffrage électronique à distance, après inscription par exemple. Ces deux possibilités nécessitent que soient résolus les problèmes d'identification et d'authentification à distance par

voie électronique, ce qui demandera encore de très importants efforts. En conséquence, la norme prévoit que l'on envisage d'instaurer des procédures d'inscription en ligne.

III. Candidats

Norme n° 43. «Une liste de candidats produite…»

84. Afin d'offrir aux électeurs les options de vote en présence, des listes de candidats sont établies, qui recensent tous les candidats, groupements de candidats ou partis politiques en lice. Ces listes seront rendues publiques de différentes manières. La méthode la plus fréquente sera la diffusion de listes sur papier. L'utilisation des nouveaux médias tels que l'Internet pour diffuser ces informations cruciales est un moyen d'atteindre un cercle d'électeurs plus large. Naturellement, Internet ne saurait être le seul canal de diffusion employé à cette fin. En vue de son utilisation, il convient de s'assurer que les listes de candidats sont complètes, exactes et authentiques, et que des mesures techniques adéquates ont été prises à cet effet. Cela implique l'utilisation de signatures numériques et la certification du site web selon une procédure adéquate.

85. Dans le contexte du vote électronique local, l'information contenue dans les machines à voter installées dans les bureaux de vote reproduira selon toute probabilité l'ensemble des indications imprimées sur les bulletins en papier. Pour certains types de machines à voter, cette information figurera sur un support matériel tel que des boutons physiques que l'électeur pourra presser. Pour d'autres, elle sera affichée par voie numérique ; on peut dans ce cas parler d'un bulletin de vote électronique.

IV. Vote

Norme n° 44. «Lorsque le vote électronique à distance se déroule pendant l'ouverture des bureaux de vote, il conviendra tout particulièrement…»

86. Le système de vérification des noms des électeurs doit être actualisé en permanence en ce qui concerne les personnes qui ont déjà exprimé leur suffrage. Toutefois, si certains électeurs n'ont le droit de voter que dans le bureau de vote et qu'une liste distincte a été établie pour eux, la liste électorale du système de vote électronique à distance n'a pas besoin d'être mise à jour en ce qui concerne ces électeurs. En pareil cas, d'autres méthodes peuvent être requises pour empêcher que les électeurs ne s'expriment à la fois dans un bureau de vote et par l'autre moyen disponible.

87. 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 les plages de temps pour le vote électronique à distance. De prime abord, il semblerait logique que les périodes soient les mêmes pour les deux méthodes, afin d'éviter les complications et les distinctions. Toutefois, voici deux considérations, parmi d'autres, qui militent en faveur de périodes différentes :

– lorsque le dépôt d'un bulletin dans un bureau de vote est l'option de repli pour les électeurs qui se trouvent sur le territoire national de la consultation, il peut arriver, en cas de panne du système de vote électronique, que la clôture du moyen de vote électronique doive intervenir avant celle du bureau de vote.

– lorsque le système est conçu et mis en œuvre de telle façon que les électeurs peuvent choisir entre les deux modes sans inscription préalable et que les modes utilisés ne disposent pas d'une liste commune qui indiquerait quels électeurs ont déjà exprimé leur suffrage, il convient, d'une manière générale, d'éviter tout chevauchement entre les plages de temps pendant lesquelles ces modes sont disponibles.

88. Quel que soit le résultat de ces considérations architecturales, le décompte ne doit commencer qu'après la clôture de tous les modes de suffrage.

Norme n° 45. «Le vote électronique à distance pourra commencer et se terminer avant...»

89. 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. L'objectif d'une telle mesure peut être notamment d'offrir aux citoyens une accessibilité et une qualité de service accrues.

90. Toutefois, le vote électronique à distance ne devrait pas se poursuivre après la fermeture des bureaux de vote. En cas d'indisponibilité du système de vote électronique (par exemple dans le cas d'un ordinateur hors service à la suite d'une panne de courant), un électeur présent sur le territoire national devrait encore avoir la possibilité de 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. Toutefois, l'expérience amènera peut-être à conclure à l'inutilité de la présente recommandation relative à l'heure à laquelle le vote électronique doit prendre fin. C'est un des points qui pourront être réexaminés quand le Conseil de l'Europe se penchera sur l'impact de cette recommandation, et il serait utile que les Etats membres intègrent également aux rapports qu'ils feront sur le vote électronique ou la mise en œuvre de celui-ci toute expérience qu'ils auraient faite en la matière.

91. Afin de tenir compte d'éventuels retards dans la transmission de l'information électronique, l'acceptation des bulletins électroniques déposés avant la clôture du vote électronique peut être prolongée pour une courte durée au-delà de la clôture du vote électronique (voir la norme n° 96, annexe III de la recommandation).

Norme n° 46. «Pour chaque mode de suffrage électronique, des modalités d'aide et d'assistance...»

92. Des modalités d'aide et d'assistance sur les procédures de vote devront être établies et disponibles quel que soit le mode de suffrage employé. Il convient que ces modalités soient accessibles au moins par la même voie pour chacun des modes de suffrage électronique. Dans le contexte du vote par l'Internet, l'assistance doit donc être accessible par le biais d'un site web et du courrier électronique. Pour le vote par téléphone, un système d'assistance téléphonique sera mis en place. En outre, des solutions de rechange seront prévues pour le cas où l'indisponibilité d'un mode de suffrage électronique à distance obligerait les électeurs à en changer. Un service d'assistance téléphonique devrait ainsi accompagner les systèmes de vote électronique à distance sur l'Internet.

93. Les modalités d'aide et d'assistance ne devraient pas mettre en danger le secret du vote.

Norme n° 47. «Toutes les options de vote seront présentées de manière égale...»

94. L'électeur doit pouvoir accéder avec la même facilité à toutes les options de vote. L'égalité de la présentation ne peut être possible ou appropriée entre les différents modes. Les écrans de téléphone portable, de télévision numérique ou de PC présentent l'information de manière différente.

95. Il faut être conscient du fait que, si la question de la disposition des noms des candidats sur un écran semble être de nature technique, elle ne peut pour autant être confiée aux techniciens qui conçoivent un système de vote électronique.

96. Il est également nécessaire, par souci d'égalité, de prévoir des mesures tendant à prévenir toute omission d'une information devant figurer sur le bulletin électronique. En l'absence de telles mesures, le résultat de la consultation électorale ou référendaire risquerait d'être affecté, car une option de vote aurait manqué sur les bulletins électroniques ou certains d'entre eux.

Norme n° 48. «Le bulletin électronique servant…»

97. Lors de l'émission du vote, l'environnement immédiat de l'électeur devrait être dépourvu de tout objet ou information susceptible d'influencer son choix de manière partisane. En ce qui concerne le vote par l'Internet, cet environnement inclut en particulier les écrans qui s'affichent sur l'ordinateur de l'électeur lorsqu'il accède au site web de vote électronique. Ces écrans ne devraient pas contenir davantage d'informations relatives aux options en présence que les bulletins papier. Cela concerne par exemple les fenêtres qui se superposent à la page visitée *(pop-up)* pour promouvoir un candidat, ou les éléments audio associés à un candidat ou à un point de vue particulier.

98. Les mots «autres messages» désignent des messages partisans susceptibles d'influencer l'électeur, autres que les messages autorisés par les dispositions législatives internes. Cela n'interdit pas, par exemple, l'affichage d'informations officielles sur les options de vote.

Norme n° 49. «S'il est décidé de permettre l'accès à des informations sur les options de vote…»

99. Cette norme n'est pas contraire à la précédente. Elle traite du processus décisionnel, tandis que la précédente concerne le processus de dépôt de bulletin.

Norme n° 50. «L'attention des électeurs utilisant un système de vote électronique sera…»

100. Actuellement, le vote en ligne n'est pas de pratique courante. Si l'attention des électeurs n'est pas suffisamment attirée sur le fait que le vote par l'Internet est un vote réel, ceux-ci pourraient avoir l'impression de participer à une élection factice ou à un test. Inversement, des mesures analogues doivent être prises pour que les participants à des votes organisés à des fins de démonstration ou de test ne s'imaginent pas avoir réellement voté. Il faut également prévoir le risque de confusion entre une élection et un sondage d'opinion.

Normes nos 51 et 52. «Dans un environnement supervisé…»

101. Dans un environnement surveillé, le système de vote électronique devrait inclure une parade en cas de disparition d'une information qui pourrait servir à prouver le contenu du bulletin déposé. Si la législation électorale nationale exige que le système de vote électronique remette à l'électeur une preuve papier du suffrage exprimé, cette preuve doit être soumise aux mêmes conditions de secret qu'un bulletin papier. L'électeur ne doit pas pouvoir montrer cette preuve à autrui, ni la retirer du bureau de vote. Par exemple, l'électeur pourrait être obligé

de déposer la preuve papier dans une boîte dans le bureau de vote ou dans un appareil qui la détruirait.

102. Dans un système de vote électronique à distance utilisant l'Internet, l'électeur doit pouvoir supprimer, sur le support utilisé pour voter, les informations concernant son vote. L'une des manières les plus courantes d'utiliser l'Internet met à contribution un logiciel de navigation sur la machine à voter, et un serveur (du côté des membres du service électoral) ; or, l'une des caractéristiques de ce dispositif, c'est le fait que l'affichage et le stockage des informations liées à l'électeur ne peuvent être entièrement contrôlés par le serveur. D'où la nécessité d'être particulièrement attentif à la manière dont sont assurés, dans les systèmes de vote électronique, le secret et l'anonymat du vote. Il y a au moins trois niveaux à prendre en considération. Le premier est celui de l'application web. Le deuxième est celui du logiciel de navigation. Enfin, le troisième niveau est celui du logiciel de travail sur l'ordinateur de l'électeur.

Au niveau de l'application web, il ne faudrait pas que l'utilisateur puisse conserver une copie de son vote. Cela signifie que l'application ne doit pas proposer les fonctions d'impression, de sauvegarde ou de stockage du vote sur l'écran ni la partie d'écran où le vote est visible.

De même, le logiciel de navigation ne devrait pas proposer d'option permettant d'imprimer l'écran sur lequel le vote est visible. Il convient de noter que les logiciels de navigation peuvent conserver les informations de plusieurs manières. Par exemple, en utilisant le bouton « En arrière » d'un logiciel de navigation, on peut afficher un ou plusieurs écrans précédents. Cette fonctionnalité générique des navigateurs devrait être, autant que possible, désactivée par l'application web. Une exigence minimale voudrait qu'il n'y ait pas de stockage des informations après que l'électeur a déposé son bulletin.

Le troisième niveau est celui des logiciels qui peuvent enregistrer d'une façon ou d'une autre les opérations effectuées par tel utilisateur d'un ordinateur. Voici trois exemples relativement courants : les utilitaires de capture d'écran ; les utilitaires d'enregistrement de séquences d'écran ; les utilitaires d'enregistrement des touches frappées par l'utilisateur. Il peut se faire que le système de vote électronique n'ait pas la capacité d'empêcher l'utilisation de tels logiciels.

Norme n° 55. « Tout décodage nécessaire au dépouillement… »

103. Le cryptage des bulletins peut être nécessaire pour assurer l'anonymat du vote. Très souvent le bulletin est crypté avant le début de la transmission par les réseaux ; il est conservé crypté dans l'urne et il est décodé avant le dépouille-

ment. Celui-ci est effectué avec des bulletins décodés, qui ne peuvent être mis en corrélation avec tel ou tel électeur.

104. Toutefois, il existe des méthodes de cryptage avec lesquelles il n'est pas nécessaire de procéder au décodage avant le dépouillement (cryptage homomorphique). Le dépouillement peut 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.

Annexe III

Exigences techniques

Introduction aux exigences techniques

105. Les systèmes électroniques peuvent être utilisés pour faciliter une ou plusieurs des différentes étapes d'une élection ou d'un référendum. Lorsque leur utilisation est envisagée dans de telles circonstances, il est nécessaire de s'assurer qu'ils fonctionnent parfaitement et totalement. A cette fin, le présent document contient un ensemble de normes techniques destinées à aider ceux qui souhaitent mettre en place de tels systèmes.

106. Il se peut que les étapes d'une élection ou d'un référendum donné ne soient pas toutes couvertes par des dispositifs électroniques. Il est donc important que les fonctionnalités soient organisées de manière à ce que les principales phases de l'élection ou du référendum soient mises en œuvre en tant qu'unités distinctes.

107. Traditionnellement, ces étapes essentielles sont les suivantes :

– annonce de l'élection ou du référendum ;

– inscription des électeurs ;

– désignation et enregistrement des candidats, ou détermination des options du référendum ;

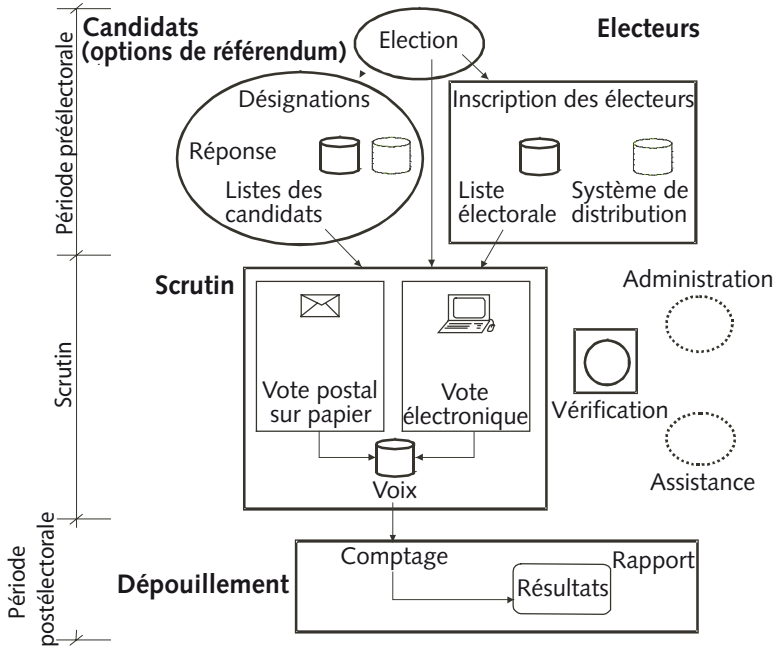
– vote ;

– dépouillement ;

– proclamation des résultats ;

– vérification.

Figure 1 : Modèle des processus EML (simplifié ; extrait de EML v4.0a*, figure 2B)*



108. La liste ci-dessous contient les éléments essentiels d'un mécanisme électoral ou référendaire qu'il convient d'organiser de telle sorte qu'il soit facile de faire le parallèle avec leurs équivalents traditionnels. Ce sont :

– la liste électorale ;
– la liste des candidats ou la liste d'options (dans laquelle l'électeur peut faire son choix) ;
– l'urne électronique ;
– le dépouillement.

109. Les normes techniques se divisent en six thèmes différents : l'accessibilité, l'interopérabilité, le fonctionnement des systèmes, la sécurité, la vérification, l'homologation et la durabilité. Chacun de ces thèmes est présenté de façon détaillée dans un chapitre distinct de la recommandation et de l'exposé des motifs. Le dernier, l'homologation, est suivi d'une description de la méthodologie d'analyse des risques.

A. Accessibilité

Norme n° 61. «Des mesures seront prises pour garantir…»

110. Pour garantir l'accessibilité et la facilité d'utilisation des systèmes d'élection électronique, il faut envisager les différents problèmes que les utilisateurs pourraient rencontrer du fait d'un handicap, de leur âge, de leur langue ou de leur mode de vie.

111. Ainsi, les personnes souffrant de divers troubles de la vue, d'une part, ou de dyslexie d'autre part, apprécieront des dispositifs de lecture d'écran, un fort contraste entre le texte et le fond, ainsi que la possibilité de modifier le texte dans leur navigateur Internet ou dans la machine de vote. Les utilisateurs atteints de troubles de la communication peuvent préférer des informations présentées de manière graphique. Ceux qui ont des troubles de la coordination préfèrent le clavier à la souris. Les kiosques doivent être adaptés aux besoins des personnes à mobilité réduite.

112. Des instructions appropriées seront remises aux électeurs; elles doivent être faciles à comprendre et à suivre.

Norme n° 62. «Les utilisateurs seront impliqués dans la conception des systèmes de vote électronique…»

113. L'accessibilité des systèmes de vote électronique implique qu'ils soient conçus de manière à ce qu'autant d'électeurs que possible, et à terme tous les électeurs, puissent les utiliser.

114. Les produits et les services doivent être fonctionnels, dûment adaptés à la tranche d'âge et aux besoins du public concerné, mais sans particularités inutilement compliquées ou chères qui ne présenteraient qu'un intérêt limité.

115. Ces deux normes peuvent être atteintes grâce à une bonne collaboration entre l'équipe conceptrice et un panel d'utilisateurs.

Norme n° 63. «Les utilisateurs se verront offrir… des fonctions complémentaires…»

116. Le Consortium du World Wide Web (W3C) a été créé en octobre 1994 pour amener le Web mondial à son potentiel maximal au moyen de protocoles communs élaborés pour favoriser son évolution et garantir son interopérabilité. Le W3C compte environ quatre cents organisations membres partout dans le monde et jouit d'une reconnaissance internationale pour son rôle dans l'expansion du Web. Le W3C développe des technologies interopérables (spécifications,

lignes directrices, logiciels et outils) ; c'est un forum d'information, d'échanges, de communication et de conceptions communes.

117. En vue de promouvoir un haut degré d'accessibilité au profit des personnes handicapées, le W3C a lancé l'Initiative d'accès au Web (WAI). En coordination avec différentes organisations dans le monde, la WAI vise à instaurer une accessibilité plus grande du Web à travers cinq principaux domaines d'action : la technologie, les lignes directrices, les outils, la formation et l'élargissement du cercle des utilisateurs, et la recherche et développement. La WAI a déjà produit un ensemble de normes et de lignes directrices en faveur de l'accessibilité (par exemple, lignes directrices sur l'accessibilité des contenus du Web, des outils de création de sites, des agents utilisateurs, du langage XML, etc.). Pour de plus amples renseignements, veuillez consulter le site Internet de la WAI à l'adresse : http ://www.w3.org/WAI.

Norme n° 64. «…il conviendra de veiller à leur compatibilité avec les produits existants…»

118. Lorsqu'on développe des systèmes, on constate régulièrement qu'une nouvelle version peut être si différente de la précédente qu'elles sont incompatibles. Pour éviter une telle situation, un programme de test doit être mis en œuvre à chaque modification du système. Il serait même indiqué de dresser et de tenir à jour une liste des systèmes, produits et équipements spécifiques compatibles.

Norme n° 65. «La présentation des options de vote sera optimisée pour l'électeur.»

119. Il faut que les produits et services puissent être adaptés aux restrictions fonctionnelles et aux circonstances spécifiques à l'utilisateur sans porter atteinte au principe d'égalité. Cela peut se traduire par l'offre de versions différentes d'un même produit, par des modifications des paramètres clés, par une conception modulaire, par des appareils auxiliaires ou d'autres moyens.

B. Interopérabilité

Norme n° 66. «Des normes ouvertes seront utilisées…»

120. Afin de permettre le recours aux systèmes ou services de vote électronique de différents fournisseurs, ce qui implique une interopérabilité entre ces divers systèmes ou services. L'interopérabilité exige que les entrées et sorties soient conformes à des normes ouvertes et en particulier à des normes ouvertes en matière de vote électronique.

121. Le fait de recourir à ce type de normes offre les principaux avantages suivants :

– elles offrent un choix plus vaste en termes de produits et de fournisseurs ;

– elles assurent une dépendance moindre vis-à-vis d'un seul fournisseur ;

– elles permettent d'éviter le blocage par des systèmes propriétaires ;

– elles offrent une stabilité ou une réduction des coûts ;

– elles s'accommodent plus facilement de modifications ultérieures.

Norme n° 67. « Actuellement, l'EML (Election Markup Language)*… »*

122. L'Organisation pour l'avancement des standards d'information structurée (OASIS), a constitué au printemps 2001 un comité technique sur les services relatifs aux élections et au vote, chargé de définir des normes pour les informations sur les services relatifs aux élections et au vote fondées sur le langage XML. Des informations complémentaires sur la composition et les travaux de ce comité sont disponibles à l'adresse http ://www.oasis-open.org/committees/election.

123. Le langage de balisage pour les élections ou *Election Markup Language* (EML), la première spécification XML de ce type, est actuellement la seule norme d'échanges structurés de données entre les moyens, matériels et logiciels, et les fournisseurs de services intervenant d'une manière ou d'une autre dans la fourniture de services d'aide aux élections ou aux électeurs. Sa fonction est la définition d'interfaces ouvertes, sûres, normalisées et interopérables entre les différents éléments des systèmes électoraux. L'EML est un ensemble de données et de définitions de messages décrit comme un ensemble de schémas XML. Il évolue en permanence pour répondre aux besoins des différents systèmes de vote. La version la plus récente disponible à l'heure de l'adoption de la recommandation sert de référence à tous les Etats membres qui souhaitent recourir à un système de vote électronique. La façon dont cette version de référence sera mise à jour dans l'avenir devrait être précisée.

124. Etant donné que l'évolution de la technologie est imprévisible au moment de l'adoption de la recommandation, il n'est pas exclu qu'un système valable à l'époque, notamment l'EML, puisse un jour ne plus être le système le plus approprié pour des élections ou des référendums électroniques, et donc ne plus être utilisé par un pays ou un groupe de pays.

Norme n° 68. « Les besoins spécifiques en matière de données électorales ou référendaires… »

125. Etant donné que les dispositions électorales varient d'un pays à l'autre, on doit prévoir la possibilité d'adapter la norme aux nécessités locales. L'EML, basé

sur la technologie XML, prévoit une procédure d'adaptation aux circonstances locales qui permet de recourir par exemple à des données supplémentaires ou une structure particulière. Il existe plusieurs méthodes d'adaptation du schéma XML aux paramètres locaux, par exemple le Schematron. Il faut veiller à ce qu'une telle «localisation» n'empêche pas un module équivalent d'un autre fournisseur de fonctionner dans l'environnement ainsi adapté aux paramètres locaux.

C. Fonctionnement des systèmes

126. Cette section se réfère à l'équipement, l'infrastructure et les logiciels fonctionnant dans un environnement contrôlé. Cela inclut les serveurs, les dispositifs de communication, les appareils en libre service, leur système d'exploitation et d'autres types de logiciels. Cela exclut les appareils personnels des électeurs comme leurs PC, leurs agendas électroniques, leurs téléphones portables et les logiciels qui y sont liés aussi bien que les équipements publics de réseaux, leurs appareils et logiciels.

Norme n° 69. «Les autorités électorales compétentes publieront …»

127. L'évolution permanente des nouvelles technologies de l'information et de la communication impose aux personnes en charge des infrastructures de demeurer en éveil et de se tenir à jour en ce qui concerne tant les équipements que les logiciels. Cela nécessite de fréquentes adaptations tant de l'infrastructure centrale que des équipements de vote utilisés dans un environnement contrôlé (machine à voter). Ces adaptations devront être certifiées selon les normes en vigueur dans chaque Etat avant de pouvoir être mises en exploitation.

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

Norme n° 70. «Les personnes en charge du fonctionnement des équipements définiront une procédure de secours…»

Norme n° 71. «Des mesures de secours suffisantes seront mises en place…»

Norme n° 72. «Les responsables de l'équipement disposeront de procédures pour garantir…»

129. Plus que tout autre système électronique à l'usage du public, ceux qui servent au vote électronique doivent avoir une fiabilité maximale. Pour cette raison, il est nécessaire de formaliser les procédures de traitement des cas particuliers et des problèmes, et de mettre en place des moyens suffisants pour pallier les incidents relatifs à l'infrastructure.

130. Les autorités électorales doivent définir un niveau de service particulier avant de mettre en route le système. Suivant le niveau à atteindre, une analyse des risques devrait être réalisée et des scénarios mis en place (procédures, mécanismes de sauvegarde, réservation de ressources, etc.).

Norme nº 73. «Avant chaque scrutin ou référendum, l'équipement sera vérifié et approuvé…»

131. Il est impossible pour l'ensemble de l'électorat d'exercer son droit à la transparence du scrutin. Il est d'autant plus important que les autorités compétentes, les partis politiques et, le cas échéant, les observateurs aient le pouvoir de faire inspecter le système en tout ou en partie par un organisme spécialisé de leur choix.

132. Il conviendrait de distinguer clairement les contrôles effectués régulièrement après chaque élection ou référendum et les contrôles réalisés chaque fois que le système est modifié à quelque égard que ce soit. Dans le premier cas, les vérifications pourraient être confiées au personnel ordinaire 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. Pour de plus amples renseignements, voir plus loin le paragraphe consacré à l'homologation.

Norme nº 74. «Toute opération technique sera soumise à une procédure officielle de contrôle…»

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

134. Les autorités électorales doivent avoir connaissance de tous les changements importants apportés au système afin d'anticiper les conséquences qui pourraient en découler et afin de choisir les mesures de communication appropriées.

Norme n° 75. «Les équipements clés du vote ou référendum électronique seront situés…»

135. Pour leur sécurité, il est particulièrement souhaitable que les systèmes centraux soient installés dans des lieux sûrs et placés sous surveillance. L'accès devrait en être restreint. Pour pouvoir réagir en cas de dégâts matériels, il convient de prévoir un lieu de substitution avec l'équipement adéquat mis en réserve à l'avance.

136. 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, clé mémoire USB, version papier) et de les stocker en plusieurs endroits.

Norme n° 76. «En cas d'incident susceptible d'affecter l'intégrité du système…»

137. Il est important que tout incident soit rapporté aux autorités compétentes, responsables d'édicter des règles de communication conformes à la législation en vigueur et de veiller à ce que les partis politiques et les citoyens soient dûment informés.

D. Sécurité

Introduction

138. De bonnes mesures de sécurité constituent un préalable indispensable à la mise en œuvre du vote électronique. Comme tout dispositif technique, un système de vote électronique est sujet aux erreurs et aux tentatives délibérées ou involontaires de contourner les mesures de sécurité. Il faut protéger le système contre toute attaque et préserver les principes cardinaux de suffrage universel, égal, libre, secret et direct. Il faut faire spécialement attention aux attaques systématiques parce qu'elles peuvent particulièrement affecter les résultats des scrutins. D'une manière générale, les élections ou référendums impliquant un recours au vote électronique doivent être aussi sûrs que les élections ou référendums qui ne font pas appel au vote électronique (voir le paragraphe i de la recommandation).

139. Les exigences techniques de sécurité de la recommandation reposent sur les pratiques acceptées en matière de sécurité des systèmes informatiques et sur

une analyse de risque (voir ci-après). Ces exigences se fondent sur les critères suivants :

– *neutralité technologique* : il s'agit d'élaborer des recommandations de sécurité technique technologiquement neutres, afin de ne pas restreindre les solutions à un groupe limité de technologies ou de modes d'expression des suffrages (en se concentrant par exemple sur l'Internet) ;

– *durabilité* : les recommandations de sécurité doivent rester valables indépendamment de l'évolution rapide de la technologie. Ce principe est étroitement lié à la neutralité technologique ;

– *méthodologie* : les pratiques et les normes acceptées doivent être suivies dans l'élaboration des recommandations de sécurité afin d'améliorer la confiance dans le résultat ;

– *polyvalence* : les recommandations doivent pouvoir s'appliquer dans les différentes formules de vote électronique, c'est-à-dire qu'elles seront applicables aux machines de vote des bureaux de vote et au vote à distance – à la fois aux kiosques de vote installés dans des environnements contrôlés et au vote électronique dans des environnements sans surveillance ;

– *EML* : les recommandations de sécurité technologique sont fondées sur le modèle des processus EML, qui sert de base aux travaux menés par le sous-groupe sur les normes techniques fondamentales.

Terminologie relative à la sécurité informatique

140. Cette section utilise souvent les expressions ci-dessous, relatives à la sécurité informatique. Leur définition est principalement tirée des normes Iso pertinentes.

Contrôle d'accès	La prévention de toute utilisation non autorisée d'une ressource (Iso 7498-2 :1989)
Authentification	La garantie de l'identité déclarée d'une entité (Iso/IEC 10181-2 :1996)
Disponibilité	Le fait d'être accessible et utilisable sur demande (TR 13335-1 :1996)

Confidentialité	Le fait de ne pas laisser disponibles ou de ne pas divulguer des informations à des personnes, des entités ou des processus non autorisés (Iso 7498-2 :1989) (TR 13335-1 :1996)
Profil de protection	Ensemble d'exigences de sécurité, indépendant de l'implémentation, pour une catégorie de produits qui couvre des besoins de sécurité spécifiques d'utilisateurs (Iso 15408).
Utilisateur ou acteur	Une entité qui est autorisée à interagir avec le système de vote électronique de manière globale ou avec un de ses composants. Cela inclut *inter alia* les électeurs, les candidats et les vérificateurs.

I. Exigences générales

Norme n° 77. «Des mesures techniques et organisationnelles seront prises…»

141. Les contrats de niveau de service (*Service level agreements* – SLA) fixent généralement des taux de disponibilité et de panne. Un certain niveau de dégradation de service peut être admissible pendant les périodes de dérangement, par exemple quand un serveur d'un réseau 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 devra toutefois envisager l'éventualité d'attaques délibérées par saturation et documenter les réserves de moyens prévues pour maintenir le fonctionnement du système. Des tests indépendants d'intrusion peuvent diminuer les chances de succès des attaques par saturation.

142. Le choix des services dont la disponibilité doit être préservée dépend de la période concernée (préélectorale, du scrutin ou postélectorale). En période préélectorale, les processus de désignation et d'inscription et les services correspondants doivent être disponibles ; en période de scrutin, ce sont les processus de vote et les services correspondants ; et en période postélectorale ce sont les processus de dépouillement et de communication des résultats et les services correspondants. Les processus de vérification doivent être opérationnels à toutes les étapes. Les limites prédéfinies des contrats de niveau de service, les taux de pannes acceptables ou les dégradations de service peuvent toutefois varier suivant les différents stades ou services.

Norme n° 78. «Le système de vote électronique préservera…»

143. Suivant les pratiques nationales, des exigences de confidentialité supplémentaires peuvent entourer les décisions de candidats. La confidentialité est alors de mise.

Norme n° 79. «Le système de vote électronique vérifiera régulièrement…»

Norme n° 80. «Le système de vote électronique restreindra l'accès…»

Norme n° 81. «Le système de vote électronique ou ses éléments protégeront les données d'authentification…»

144. Cet objectif concerne tous les sujets. Les services comme ceux qui informent les électeurs avant leur entrée dans le processus de vote, et pour lesquels l'authentification est évidemment sans objet, sortent du cadre du présent document.

Norme n° 82. «L'identification des électeurs et des candidats sera assurée…»

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

146. Etant donné que quelqu'un peut à la fois se présenter comme électeur et comme candidat, il est important que le système attribue à chaque personne une seule identification pour l'ensemble de ses rôles. L'authentification peut se fonder sur l'identité ou sur le rôle. Celle fondée sur l'identité est recommandable pour l'inscription des électeurs ou l'expression des suffrages, ou pour l'acceptation ou le rejet d'une désignation ; mais l'authentification fondée sur le rôle suffit vraisemblablement pour les administrateurs, les vérificateurs ou autres.

Norme n° 83. «Le système de vote générera des données d'observation assez détaillées et fiables…»

Norme n° 84. «Le système de vote électronique sera doté d'horloges synchronisées fiables…»

147. La précision nécessaire peut varier suivant les utilisateurs de la source de synchronisation, selon les tolérances appliquées par exemple à l'inscription et à l'enregistrement des suffrages. L'on peut donc envisager 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 pourraient suffire dans les entrées de journal. Notons toutefois que des repères temporels sur les suffrages peuvent compromettre la confidentialité du scrutin. C'est pourquoi il faut étudier avec soin s'il est opportun d'y recourir, et de quelle manière, pour les bulletins ou les suffrages.

Norme n° 85. «Les autorités électorales assumeront la responsabilité générale…»

148. Les autorités électorales sont tenues de veiller à ce que le système de vote électronique soit conforme aux normes de sécurité. La notion d'indépendance de l'organisme chargé d'évaluer le respect des normes de sécurité implique une indépendance à la fois vis-à-vis du fabricant ou du fournisseur du système et du point de vue des ingérences politiques. Cet organisme devra certifier que les mesures de sécurité technique sont effectives et correctement mises en œuvre. Il devra garantir qu'il n'a fait l'objet d'aucune influence politique indue dans son évaluation du système de vote électronique. L'organisme indépendant peut être un organisme gouvernemental tel qu'un office chargé de la certification de la sécurité informatique nationale, voire les autorités électorales elles-mêmes ; ce peut aussi être une organisation privée ou internationale comme les laboratoires d'évaluation ou les agences de certification, comme celles qui sont accréditées pour assurer les programmes nationaux ou internationaux d'évaluation tels que le BS7799/Iso17799, les Critères communs ou Itsec. La nomination d'un organisme indépendant doit se faire dans la transparence.

149. Si des profils de protection Critères communs/Iso 15408, évalués et certifiés, sont élaborés sur la base de cette recommandation de sécurité, une évaluation indépendante est réalisée dans le cadre du programme des Critères communs.

II. Exigences en période préélectorale

Norme n° 86. «L'authenticité, la disponibilité et l'intégrité des listes électorales…»

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

Norme n° 87. «Il sera possible d'établir si la désignation des candidats…»

151. Cela peut par exemple être assuré par horodatage ou par la confirmation d'un système fiable.

Norme n° 88. «Il sera possible d'établir si l'inscription des électeurs…»

152. Cela peut par exemple être assuré par horodatage ou par la confirmation d'un système fiable.

III. Exigences pendant la période du scrutin

Norme n° 89. «L'intégrité des données communiquées à partir de la période préélectorale…»

153. Les données nécessaires en période de scrutin varient en fonction du système utilisé. Ainsi, les listes de candidats sont nécessaires pendant la période du scrutin si le bulletin est dynamiquement généré à ce stade, mais il est également possible de générer les bulletins en période préélectorale et de les communiquer pour la période du scrutin. C'est pourquoi la norme n° 89 ne dresse pas la liste des données dont l'intégrité et l'authenticité doivent être préservées, mais parle plus généralement de «données communiquées».

154. La liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme confère ce droit de vote.

N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter les suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire, cas de figure dans lequel il est essentiel de disposer d'une liste de ceux qui ont voté.

Norme n° 90. «On garantira que le système de vote électronique présente…»

155. Entre autres éventualités, il faut envisager qu'un attaquant pourrait présenter de faux systèmes par imitation d'un serveur officiel par manipulation du système de nom de domaine (DNS), par l'utilisation d'un nom de domaine similaire à celui du serveur officiel, par une attaque de type *man-in-the-middle*, ou par un cheval de Troie dans le système de l'électeur qui remplacerait le bulletin original ou injecterait de faux bulletins. Une signature électronique appliquée par les autorités électorales sur le bulletin permet de vérifier ce dernier. Cela ne doit toutefois pas engendrer une violation du secret de la décision de l'électeur.

Norme n° 91. «Il sera possible d'établir qu'un suffrage a été exprimé…»

156. Cela peut par exemple être assuré par horodatage ou par la confirmation d'un système fiable. Les informations d'horodatage ne doivent toutefois pas générer des voies suivies par l'information susceptibles de révéler le suffrage.

Norme n° 92. «Des mesures suffisantes seront prises pour assurer…»

157. Dans le cadre non surveillé du vote à distance, comme le vote par l'Internet, l'électeur ou des tiers contrôlent généralement l'environnement. Le système de vote peut difficilement contrôler l'existence d'un environnement sécurisé. Il faut veiller à préserver la confiance des utilisateurs dans les systèmes, par exemple en leur permettant de vérifier qu'ils sont en présence du logiciel authentique, ou par des recommandations indiquant comment protéger l'environnement du système.

Norme n° 93. «Les informations résiduelles qui renferment…»

158. Pendant l'expression d'un suffrage, les informations qui renferment la décision de l'électeur peuvent être conservées en divers endroits pour des raisons techniques. Ainsi, dans le cas d'un vote par l'Internet par le biais d'un PC, les données qui renferment la décision de l'électeur peuvent être enregistrées dans la mémoire du PC, dans le cache du navigateur Internet, dans la mémoire vidéo, dans les fichiers d'échange et temporaires, etc. Suivant le système, d'autres points de stockage des données doivent être pris en compte. L'expression «informations résiduelles» désigne celles qui restent accessibles en divers endroits après l'enregistrement du suffrage, et qui sont susceptibles de révéler la décision de l'électeur. Cette norme recommande aux développeurs de systèmes ou aux prestataires de services de concevoir le système de vote électronique de manière à ce que les informations soient effacées dès l'enregistrement du suffrage. Toutefois, d'un point de vue technique, c'est difficilement applicable dans le cas du vote à distance. Quoi qu'il en soit, toutes les mesures envisageables doivent être prises pour assurer la suppression de ces informations résiduelles dès l'enregistrement du suffrage.

Norme n° 94. «Le système de vote électronique vérifiera en premier lieu…»

159. Quand des jetons anonymes de vote attestent le droit de vote d'un électeur, l'authentification de ce dernier peut être facultative. Il faut cependant encore l'empêcher d'exprimer des suffrages multiples sous couvert de l'anonymat.

Norme n° 96. «A l'issue de la période du scrutin électronique…»

160. Dans les votes à distance, les services peuvent s'attendre à une charge plus importante peu avant la fermeture du scrutin. Cette surcharge peut se traduire

par des temps de transfert plus longs des suffrages exprimés vers les urnes électroniques. Les suffrages enregistrés à temps doivent toutefois être acceptés. Il convient donc que les serveurs ne se ferment pas immédiatement à l'expiration du délai si des retards de ce genre sont prévisibles.

IV. Exigences pendant la période postélectorale

Norme n° 97. «L'intégrité des données communiquées pendant la période du scrutin…»

161. L'authentification de l'origine des données peut par exemple être assurée par des signatures électroniques dans les processus entièrement informatisés. Quand l'informatisation n'est que partielle, l'authentification de l'origine des données peut aussi faire appel à des mesures de sécurité conventionnelles telles que les signatures manuelles, les cachets, les courriers, etc. Les suffrages exprimés ou les résultats partiels du dépouillement sont les avantages les plus précieux d'un scrutin. Il est donc préférable de prendre les mesures techniques qui s'imposent pour protéger ces avantages pendant le transfert.

Norme n° 98. «Le dépouillement décomptera les voix avec précision…»

162. Afin d'améliorer la confiance, il est vital que le dépouillement soit reproductible, notamment à l'aide de différents systèmes issus de sources différentes.

Norme n° 99. «Le système de vote électronique assurera la disponibilité…»

163. Les informations renfermées dans l'urne électronique doivent être préservées aussi longtemps que nécessaire pour autoriser tout nouveau dépouillement ou une contestation devant les tribunaux, ou aussi longtemps après le scrutin que l'exigent les procédures électorales de l'Etat membre concerné.

E. Audit

I. Considérations générales

Norme n° 100. «Le système d'audit sera conçu et implanté….»

Norme n° 101. «Un audit complet d'un système de vote électronique…»

164. L'audit des processus électoraux ou référendaires est la procédure permettant d'analyser les mécanismes utilisés pour collecter et compter les voix, afin de confirmer l'authenticité du résultat.

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

166. Le principal danger qui pèse sur les systèmes de vote électronique est la non-détection des attaques contre les systèmes qui affecteraient le résultat du scrutin. C'est pourquoi une surveillance indépendante et extensive de la sécurité, la vérification, les contrôles croisés et les rapports sont des éléments vitaux des environnements de vote électronique.

167. Un système d'élection électronique devrait donc prévoir des dispositifs d'audit pour chacun de ses principaux éléments (par exemple le vote et le dépouillement). Les dispositifs de vérification devraient être présents à différents niveaux du système : logique, des applications, technique.

168. Les dispositifs de vérification au niveau logique devraient principalement rendre compte de l'utilisation qui est faite du système.

169. Les dispositifs de vérification au niveau des applications devraient fournir des informations sur les activités assurées par le système afin de permettre une reconstitution de son fonctionnement.

170. Les dispositifs de vérification au niveau technique devraient fournir des indications sur les activités administrées par l'infrastructure utilisée. Il peut s'agir, par exemple, d'informations de routine sur des charges spécifiques et des dysfonctionnements du système, mais aussi d'informations spécifiques sur les signaux envoyés par un Système de détection d'intrusion (SDI) face à d'éventuelles attaques.

II. Enregistrement

Norme n° 102. «Le système d'audit sera ouvert et complet…»

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

172. Le niveau de l'EML présente de nombreux points normalisés d'interface ouverte. Les flux de données peuvent être facilement observés et surveillés à ces points d'interface. Les systèmes de vérification doivent aussi viser les interfaces

autres que celles de l'EML, comme celles avec l'infrastructure de communication, les bases de données et les fonctions de gestion du système.

173. Des règles de procédures devraient également être élaborées afin de préciser l'utilisation des systèmes de vérification pendant le fonctionnement des systèmes électoraux ou référendaires, et des procédures prédéfinies devraient être mises en place pour assurer une réaction rapide.

Norme n° 103. «Le système d'audit enregistrera les dates et les heures, les événements et les actions…»

174. Les outils automatisés et les procédures du système doivent permettre un déroulement rapide et précis de l'analyse des données et des rapports, afin que les mesures correctives puissent être prises sans tarder.

175. Le système de vérification fournira des rapports vérifiables :

– sur les contrôles croisés de données, y compris d'EML,

– sur les attaques contre le système ou le réseau,

– sur la détection d'intrusions et les rapports correspondants,

– sur les manipulations de données,

– sur les fraudes et tentatives de fraude.

176. Le système de vérification doit conserver le relevé de toutes les attaques contre le fonctionnement du système électoral ou référendaire ou contre son infrastructure de communication. Le système comprendra un dispositif de détection et de rapport de 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 faire l'objet d'une réaction immédiate.

177. Le système de vérification doit établir le relevé de tous les dépouillements et nouveaux décomptes, y compris les décisions et actions prises, ou les exceptions faites pendant le dépouillement.

III. Contrôle

Norme n° 104. «Un système d'audit permettra de surveiller l'élection…»

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

Norme n° 105. «Les informations de l'audit ne seront pas divulguées à des personnes non autorisées.»

Norme n° 106. «Le système d'audit préservera constamment l'anonymat des électeurs.»

179. Par nature, les systèmes de vérification collectent une masse d'informations (de données). Néanmoins, si trop d'informations sont conservées, la confidentialité du scrutin peut être compromise. A l'évidence, un système de vérification doit préserver à tout moment l'anonymat des électeurs, sauf quand la législation nationale prévoit spécifiquement le contraire. Les informations collectées par le système de vérification doivent donc être protégées contre les accès non autorisés.

IV. Vérification

Norme n° 107. «Le système d'audit permettra de faire le contrôle croisé et la vérification…»

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

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

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

Norme n° 108. «Un système d'audit permettra de vérifier qu'un scrutin ou référendum électronique…»

183. Le système de vérification fournira à tout observateur la possibilité d'observer directement ou indirectement l'élection ou le référendum et de vérifier que le nombre de suffrages exprimés est exact. Pour ce faire, le système doit proposer des interfaces ouvertes et normalisées assorties de moyens d'observation élaborés, dans les limites imposées par la confidentialité des suffrages.

184. Le système de vérification doit être publiquement vérifiable. Il doit pouvoir démontrer au public que les principes des élections et référendums démocratiques ont été respectés, et que le décompte ou résultat du suffrage est légitime.

185. Cela suppose la capacité de démontrer à des tiers que le décompte ou résultat du suffrage représente véritablement et équitablement les suffrages légitimes exprimés et qu'il répond aux exigences de la réglementation applicable au vote concerné.

V. Divers

Norme n° 109. «Le système d'audit sera protégé contre les attaques…»

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

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

Norme n° 110. «Les Etats membres prendront les mesures nécessaires pour garantir…»

188. Il ne suffit pas de simplement protéger les informations collectées par le système d'audit contre les accès non autorisés. Il faut également prendre des mesures légales et d'organisation à l'égard des personnes chargées du système de vérification. Par conséquent, toute personne ayant accès au système d'audit devrait faire l'objet d'une procédure d'homologation.

F. Homologation

Norme n° 111. «Les Etats membres sont invités à mettre en place des procédures d'homologation…»

189. Les responsables des élections devraient envisager le recours à des techniques allant des simples tests à une homologation formelle, afin de garantir avant le déroulement d'une élection ou d'un référendum que le système fonctionne exactement comme prévu.

190. A l'avenir, il est possible que l'on se trouve en présence de divers systèmes de vote électronique et d'une multitude d'éléments individuels. Il pourrait alors devenir très difficile pour une instance électorale de déterminer si un produit donné est prêt à l'emploi, s'il fonctionnera correctement et fournira les bons résultats. Une procédure d'homologation s'avérera précieuse dans ce domaine, car elle pourra attester l'efficacité des éléments et limitera par conséquent les vérifications nécessaires dans l'élaboration d'un système complet.

Norme n° 112. «Soucieux d'améliorer la coopération internationale…»

191. Quand leurs organismes participent aux travaux des organisations internationales qui prévoient des dispositifs de reconnaissance mutuelle, les Etats membres peuvent bénéficier de leur travail et donc réduire leurs coûts de tests et d'homologation.

Analyse des risques – méthodologie

Les recommandations ont été élaborées suivant les Critères communs (CC)/Iso 15408. L'idée est de tirer parti de l'approche méthodologique que ce système offre dans la définition des objectifs de sécurité, à l'instar des profils de protection (PP) des CC, qui permettent de décrire les impératifs de sécurité d'une manière technologiquement neutre. De plus, les CC sont un outil internationalement reconnu[1] d'évaluation de la sécurité des produits informatiques, ce qui signifie que l'adoption de cette norme permet de développer les recommandations de sécurité en PP exploitables par l'industrie.

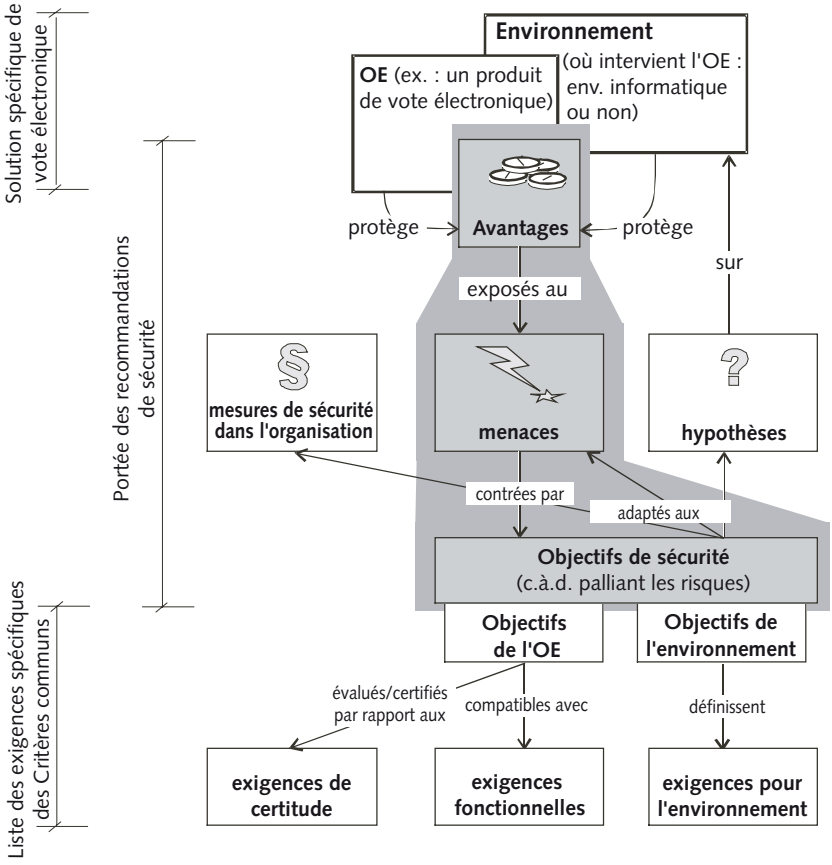
Ce document ne constitue toutefois pas un véritable PP complet, mais un «emprunt» des CC par l'utilisation de sa méthodologie afin de développer les

1. L'Accord de reconnaissance mutuelle des Critères communs a été signé par plusieurs Etats membres du Conseil de l'Europe. En juin 2004, les nations signataires de l'accord étaient l'Autriche, l'Australie, le Canada, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, Israël, l'Italie, les Pays-Bas, la Nouvelle-Zélande, la Norvège, l'Espagne, la Suède, la Turquie, le Royaume-Uni et les Etats-Unis d'Amérique.

exigences permettant d'augmenter la confiance dans le caractère complet et efficace des recommandations de sécurité technologique. Cette méthodologie est explicitée dans les paragraphes suivants.

La figure 2 ci-dessous illustre les principes de base des CC. Elle permet de présenter aux lecteurs non familiers des programmes comme les CC les idées exploitées pour élaborer les recommandations relatives à la sécurité technique. Les éléments effectivement repris dans ce document apparaissent en grisé.

Figure 2 : Synoptique de la méthodologie des Critères communs et portée du projet de recommandation de sécurité (en grisé)



Fondamentalement, les CC définissent un produit de sécurité (par exemple, un système d'élection électronique ou un de ses éléments) à évaluer comme un «objet d'évaluation» (OE). L'OE et son environnement protègent les «avantages». Une définition claire des avantages offre une bonne vision des éléments qui nécessitent une protection. Cela forme la base d'une analyse complète des menaces grâce à l'examen des avantages obtenus ou dispensés. A partir de ces menaces, des objectifs de sécurité peuvent être dégagés; une analyse permet ensuite de déterminer si les objectifs sont atteints et s'ils permettent effectivement de contrer les menaces. Cette approche définie dans les CC a aussi été utilisée dans l'élaboration des recommandations de sécurité pour le vote électronique.

A ce stade, aucune mesure d'organisation assortie des objectifs correspondants n'a été définie.

La distinction entre un produit et son environnement n'a pas été faite, ces considérations ayant été jugées trop spécifiques pour les recommandations du Conseil de l'Europe et trop liées à l'évaluation de produits concrets. Notons toutefois qu'il n'est généralement pas possible de contrer toutes les menaces par des moyens techniques – ce qui a des implications pour les CC. Ainsi, il semble virtuellement impossible d'empêcher par des moyens techniques le suffrage familial dans un scénario de vote à distance.

Le présent document n'approfondit pas davantage l'élaboration des objectifs de sécurité en relevant les exigences fonctionnelles et de certitude suivant les catalogues des CC.

En résumé, la méthodologie «empruntée» aux CC permet de définir un ensemble complet d'objectifs de sécurité aboutissant à des recommandations de sécurité. Ce document respecte diverses contraintes des CC, même s'il ne recourt qu'à certains éléments fondamentaux de ces critères. Cet aspect devrait aider les développeurs à constituer de véritables «Profils de protection» CC ou des Objectifs de sécurité, ce qui encourage de telles évaluations indépendantes des produits.

Avantages

Le modèle des processus de la figure 1 permet d'identifier les avantages suivants:

Généraux (à toutes les périodes)

1. *Données d'authentification* : les informations servant à vérifier l'identité déclarée d'un utilisateur (les données d'authentification doivent rester confidentielles).

2. *Intégrité du système* : l'authenticité du système de vote électronique ou de ses éléments qui assurent les fonctions attendues (l'intégrité du système de vote électronique ou de ses éléments doit être assurée).

3. *Vérifiabilité et observabilité* : les informations utilisées dans la vérification du bon fonctionnement du système de vote électronique ou de ses éléments ainsi que celles nécessaires à l'observation du scrutin (la disponibilité et l'intégrité des relevés de vérification des informations issues de l'observation doivent rester assurées).

Période préélectorale

1. *Décision des candidats* : la décision d'accepter ou de décliner une désignation (certaines exigences relatives à la protection de la vie privée peuvent entourer la décision de la personne désignée).

2. *Liste des candidats* : voir la définition des termes figurant dans le texte de la recommandation (la disponibilité et l'intégrité des listes de candidats doit être assurée, des règles de confidentialité peuvent intervenir jusqu'à l'acceptation ou au refus des désignations).

3. *Liste électorale* : la liste des électeurs habilités à participer à une élection ou à un référendum (l'intégrité de la liste électorale doit être assurée, et suivant les réglementations nationales des règles de confidentialité peuvent s'appliquer pour des raisons de protection de la vie privée).

4. *Processus de désignation* : le processus de désignation de listes de partis, de candidats, d'acceptation ou de refus des désignations, ou de constitution de listes d'options (la disponibilité du processus de désignation doit être préservée).

5. *Vie privée, protection des données* : le système de vote électronique contient des données à caractère personnel, telles que la liste électorale ou les décisions des candidats. Ces données ne peuvent être divulguées à des tiers non autorisés (confidentialité de la liste électorale, de la décision des candidats ; la législation applicable à la publication ou à la divulgation des listes électorales peut varier d'un pays à l'autre).

Note pour la mise en œuvre : il faut également prendre en compte les exigences de publicité (par exemple au Royaume-Uni) ou non (par exemple, au Danemark) des listes électorales. Par ailleurs, même quand les listes électorales sont considérées comme des informations publiques, le fait d'en autoriser la consultation illimitée par des moyens électroniques a des implications du point de vue de la protection de la vie privée (par exemple, parce qu'elles constituent un répertoire national des citoyens et de leurs adresses qui pourrait être exploité à des fins illégales). Il convient donc d'étudier par quel moyen l'accès public est autorisé.

6. *Processus d'inscription* : le processus d'inscription des électeurs pour élaborer les listes électorales (la disponibilité du processus d'inscription doit être préservée).

7. *Droit de vote* : le droit de l'électeur de voter – y compris la disposition l'autorisant à voter une seule fois (le droit de vote doit être préservé).

8. *Période de désignation* : la période pendant laquelle une désignation peut intervenir (le fait qu'une désignation ait pris effet dans les délais prescrits doit être vérifiable).

9. *Période d'inscription* : la période pendant laquelle une inscription peut intervenir (le fait qu'une inscription ait été effectuée dans les délais prescrits doit être vérifiable).

Période du scrutin

1. *Bulletin* : voir la définition donnée dans la recommandation (il faut présenter le bon bulletin à l'électeur, l'intégrité du bulletin doit être préservée).

2. *Liste des candidats (si nécessaire, par exemple pour générer le bulletin)* : communiquée à l'issue de la période préélectorale (voir *Période préélectorale* ci-dessus), voir la définition donnée dans la recommandation (la disponibilité et l'intégrité de la liste des candidats doivent être préservées).

3. *Suffrage* : se référer à la recommandation pour la définition (la disponibilité, l'intégrité et la confidentialité des suffrages exprimés doivent être préservées jusqu'au dépouillement et au-delà, dans l'éventualité de nouveaux décomptes).

4. *Listes électorales* : communiquées à l'issue de la période préélectorale (voir *Période préélectorale* ci-dessus). La liste des électeurs habilités à participer à un scrutin ou à un référendum (l'intégrité des listes électorales doit être assurée ; certaines législations nationales imposent des exigences de confidentialité pour protéger la vie privée).

Note pour la mise en œuvre : la liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme confère ce droit de vote.

N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter les suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire.

5. *Droit de vote* : le droit de l'électeur de voter – y compris la disposition lui permettant de voter une seule fois (le droit de vote doit être préservé).

6. *Période du scrutin* : voir la définition donnée dans la recommandation (le fait qu'un suffrage ait été exprimé pendant la période du scrutin doit être vérifiable).

7. *Décision de l'électeur*: la décision de l'électeur, entrée dans le système d'élection électronique et représentée par le suffrage. L'identité de l'électeur ne doit pas pouvoir être obtenue à partir du suffrage (la décision de l'électeur doit

rester un secret inviolable à l'examen d'un suffrage ; la confidentialité et l'intégrité de la décision de l'électeur doivent être préservées).

Note pour la mise en œuvre : la confidentialité de la décision de l'électeur doit être protégée, mais d'autres données peuvent apparaître pendant et après l'enregistrement du vote.

8. *Vie privée de l'électeur, protection des données* : le système de vote électronique renferme des données à caractère personnel de l'électeur, comme la liste électorale. Ces données ne doivent pas être révélées à des tiers (confidentialité de la liste électorale ; la législation applicable à la publication ou à la divulgation des listes électorales peut varier d'un pays à l'autre).

Note pour la mise en œuvre : il faut également prendre en compte les exigences de publicité (par exemple, au Royaume-Uni) ou non (par exemple, au Danemark) des listes électorales. Par ailleurs, même quand les listes électorales sont considérées comme des informations publiques, le fait d'en autoriser la consultation illimitée par des moyens électroniques a des implications du point de vue de la protection de la vie privée (par exemple, parce qu'elles constituent un répertoire national des citoyens et de leurs adresses qui pourrait être exploité à des fins illégales). Il convient donc d'étudier par quel moyen l'accès public est autorisé.

9. *Enregistrement d'un suffrage* : la démarche d'une personne qui exprime un suffrage (l'accès au processus de vote doit être préservé).

Période postélectorale

1. *Liste des candidats (si nécessaire, par exemple pour générer les résultats ou le rapport des élections)* : communiquée à l'issue de la période préélectorale (voir *Période préélectorale* ci-dessus), voir la définition donnée dans la recommandation (la disponibilité et l'intégrité de la liste des candidats doivent être préservées).

2. *Suffrage* : communiqué à l'issue de la période électorale, se référer à la recommandation pour la définition (voir Période électorale ci-dessus). Les principaux avantages sont les suffrages exprimés (la disponibilité, l'intégrité et la confidentialité des suffrages exprimés doivent être assurées jusqu'au dépouillement et au-delà, dans l'éventualité de nouveaux décomptes).

3. *Dépouillement* : le processus par lequel les votes sont convertis en résultat d'un scrutin (la disponibilité du dépouillement doit être préservée).

4. *Rapport des élections*: le rapport généré par le système d'élection électronique (l'intégrité du rapport doit être assurée).

5. *Résultat du décompte*: établir le résultat d'un scrutin et prévenir l'établissement prématuré de résultats partiels (le décompte doit être correct et dans les temps, et l'intégrité du résultat doit être préservée).

6. *Processus de rapport* : le processus de production d'un rapport d'élection (la disponibilité du processus de rapport doit être préservée).

Sujet	**Définition**
Administrateur	Personne assurant l'initialisation, le fonctionnement et d'autres fonctions administratives dans le système de vote électronique.
Vérificateur	Personne interne ou externe chargée d'évaluer la condition, la fiabilité et la sécurité du système de vote électronique (identifiée comme personne habilitée à entrer dans les listes de contrôle).
Autorité	Entité, personne ou processus autorisé(e) par les autorités électorales (s'identifie avant les événements liés au vote tels que le lancement d'un scrutin, la production de listes électorales, la production de résultats, etc.).
Candidat	Une option de vote constituée par une personne et/ou un groupe de personnes et/ou un parti politique
Observateur	Une personne autorisée à observer une élection ou un référendum (s'identifie en qualité d'observatrice)
Proposant	Un utilisateur (personne, groupe, organisme tel qu'un parti politique, autorité) qui désigne un ou plusieurs candidats (s'identifie comme utilisateur habilité à désigner des candidats).
Electeur	Personne habilitée à voter dans une élection ou un référendum donnés.
Menace	**Définition**
Agresseur	Personne ou processus interne ou externe qui entreprend une attaque contre le système de vote électronique ou certains de ses éléments. Personne dûment identifiée mais sortant de ses attributions (attaque interne, par exemple un administrateur qui tente d'accéder à la décision d'un électeur). L'objectif premier d'un agresseur est d'obtenir, de modifier ou d'insérer des informations sensibles ou de perturber les services.
Dysfonctionnement	Incident extérieur qui perturbe les services ou panne interne du système de vote électronique ou de ses services.

Menaces

Cette section décrit les menaces qui pèsent sur les avantages. Ces menaces sont envisagées pour chacune des étapes préélectorale, du scrutin et postélectorale telles que définies dans le modèle des processus EML, voir la figure 1. Cette démarche introduit une certaine modularité qui permet d'étudier l'analyse des menaces pour chacune des étapes du processus. Les menaces générales communes à toutes les étapes sont regroupées dans une section séparée. Une note identifie les menaces communes à deux étapes du processus.

Générales (toutes les périodes)

T.Audit_Forgery – *Falsification des données de vérification*

Un agresseur génère, modifie, insère ou supprime des données de vérification. Cela porte atteinte à la vérifiabilité et à l'observabilité.
Note pour la mise en œuvre : l'audit fait l'objet d'une section spécifique de l'annexe III ainsi que d'une autre dans le présent exposé des motifs.

T.Auth_Disclose – *Divulgation de données d'authentification*

Un agresseur accède aux données d'authentification, ce qui lui permet d'agir au nom d'un utilisateur légitime (administrateur, vérificateur, autorité, candidat, observateur, proposant, électeur) du système d'élection électronique.

T.Hack – *Piratage du système d'élection ou de référendum électroniques*

Un agresseur, interne ou externe, agit sur le système d'élection électronique, ses interfaces ou certains de ses éléments pour en exploiter des points faibles. Cela peut arbitrairement menacer la sécurité et affecte tous les avantages.
Note pour la mise en œuvre : le piratage désigne généralement des agresseurs extérieurs qui tentent de percer les protections d'un système. Dans le présent contexte, l'agresseur est toutefois envisagé comme interne ou externe car un utilisateur dûment identifié comme un administrateur, mais sortant du cadre de ses attributions, peut aussi exploiter des failles.

T.Observ_Forgery – *Falsification de données d'observation*

Un agresseur génère, modifie, insère ou supprime des données d'observation. Cela porte atteinte à la vérifiabilité et à l'observabilité.

T.System_Forgery – *Falsification de composants du système*

Un agresseur remplace le système d'élection électronique ou certains de ses éléments par des éléments contrefaits ou présente de faux éléments comme appartenant réellement au système. Cette manœuvre menace l'intégrité du système, mais peut également provoquer une remise en cause arbitraire des avantages.

Note pour la mise en œuvre : cette menace devient aussi critique si, dans un scénario de vote électronique à distance, l'attaquant déroute l'électeur vers de faux systèmes, comme des serveurs de vote par l'Internet ressemblant aux serveurs originaux et officiels. Il peut, par exemple, contrôler le service de nom de domaine (DNS) et dévier les connexions destinées à un serveur officiel – par exemple www.voting.official.at – vers une autre adresse Internet. La situation est comparable quand l'agresseur possède un nom de domaine dont l'orthographe est très proche – par exemple www.voting.oficial.at (ici, seul un « f » manque).

Période préélectorale

T.CandList_Disclose – *Divulgation d'informations relatives à la liste des candidats*

Un agresseur accède prématurément à la liste des candidats ou à certains de ses éléments, ou à la décision d'un candidat.
Note pour la mise en œuvre : les exigences en matière de publicité de la décision des candidats peuvent varier d'un pays à l'autre.

T.CandList_Modify – *Usurper une identité au cours de la désignation des candidats*

Un agresseur usurpe la place d'un proposant qui désigne un candidat. Un agresseur usurpe l'identité d'un candidat qui accepte ou refuse une désignation. Un agresseur modifie ou efface la liste des candidats.

T.Malfunction_pre – *Dysfonctionnement des systèmes ou services en période préélectorale*

Un dysfonctionnement détruit irrémédiablement la liste des candidats, la liste électorale ou les services proposés dans le processus de désignation ou d'inscription. La destruction de la liste électorale porte également atteinte au droit de vote.

T.Nomin_DOS – *Attaque par saturation contre le processus de désignation*

Un agresseur interrompt le processus de désignation ou ses services, et la disponibilité du processus pendant la période de désignation n'est plus assurée. Un agresseur empêche la génération de la liste des candidats. L'interruption de ce service affecte également la possibilité des candidats de faire connaître leur décision.

T.Nomin_Time – *Manipulation de la période/de l'heure de désignation*

Un agresseur met hors service la source de synchronisation du processus de désignation ou modifie la date et l'heure à laquelle une désignation est intervenue soit pour faire accepter une désignation réalisée en dehors de la période de désignation, soit pour disqualifier une désignation réalisée pendant cette période. L'atteinte vise la période de désignation, la liste des candidats ou l'aptitude d'un candidat à prendre sa décision dans les délais prescrits.

T.Privacy – *Divulgation de données à caractère personnel*

Un agresseur divulgue des données à caractère personnel des électeurs ou des candidats.
Note pour la mise en œuvre : la législation applicable à la publication ou à la divulgation des listes électorales ou des décisions de candidats peut varier d'un pays à l'autre.

T.Registr_DOS – *Attaque par saturation contre le processus d'inscription*

Un agresseur interrompt le processus d'inscription ou ses services, et la disponibilité du processus n'est donc plus assurée pendant la période d'inscription. Un agresseur empêche la génération des listes électorales. Cela porte également atteinte au droit de vote.

T.Registr_Time – *Manipulation de la période/de l'heure d'inscription*

Un agresseur met hors service la source de synchronisation du processus d'inscription ou modifie la date et l'heure à laquelle une inscription est intervenue soit pour faire accepter une inscription réalisée en dehors de la période d'inscription, soit pour disqualifier une inscription réalisée dans les délais. L'atteinte vise les dates et heures de cette période, la liste électorale et le droit de vote.

T.VotReg_Disclose – *Divulgation d'informations des listes électorales*

Un agresseur prend connaissance de la totalité ou de parties de la liste électorale.
Note pour la mise en œuvre : les exigences nationales peuvent varier quant aux entités habilitées à consulter la liste électorale ou quant à la confidentialité de cette liste proprement dite.

T.VotReg_Modify – *Usurpation d'identité à l'inscription des électeurs*

Un agresseur usurpe la place d'une entité habilitée à être inscrite en vue de participer à un vote, et inscrit ou efface des électeurs. Un agresseur modifie ou efface la liste électorale. Cela porte également atteinte au droit de vote.

Période du scrutin

T.Ballot_Forgery – *Falsification du bulletin de vote*

Un agresseur falsifie le bulletin de vote qui renferme la décision de l'électeur ou présente un faux bulletin de vote à l'électeur. Cela affecte également le suffrage exprimé, une décision non souhaitée intervenant dans le scrutin.

T.CandList_Modify – voir *Période préélectorale*

Cette menace existe si la liste des candidats est nécessaire pendant la période du scrutin, par exemple pour générer le bulletin de vote. Si ce bulletin de vote est généré à partir d'une liste des candidats falsifiée ou modifiée, le suffrage et la

décision de l'électeur sont affectés, car un bulletin de vote falsifié est généré (voir T.Ballot_Forgery)

T.CommD_Avail_pre – *Disponibilité/Intégrité des données issues de la période préélectorale*

Un agresseur modifie ou interrompt le flux de données communiquées depuis la période préélectorale. Il en résulte une falsification ou la disparition de la liste des candidats ou des listes électorales pendant la période du scrutin. Une liste électorale modifiée affecte le droit de vote de l'électeur.
Subtilité : la menace existe si une liste des candidats ou d'options est nécessaire pendant la période du scrutin, par exemple pour générer le bulletin de vote.
Subtilité : la menace existe si le bulletin de vote est généré à partir de la liste des candidats falsifiée ou modifiée ; le suffrage exprimé et la décision de l'électeur sont affectés, car un bulletin de vote falsifié est généré (voir T.Ballot_Forgery).
Note pour la mise en œuvre : la liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme atteste le droit de vote.
N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter l'expression de suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire.

T.CommD_Sec_pre – *Confidentialité des données communiquées*

Un agresseur prend connaissance de listes électorales communiquées.
Note pour la mise en œuvre : la réglementation qui définit quels intervenants peuvent avoir accès à la liste électorale varie d'un pays à l'autre ; parfois celle-ci n'a aucun caractère confidentiel[1].
Note pour la mise en œuvre : la liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme atteste le droit de vote.
N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter l'expression de suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire.

T.Malfunction_elect – *Dysfonctionnement des systèmes ou services pendant le scrutin*

Un dysfonctionnement détruit irrémédiablement la liste des candidats, la liste électorale, des suffrages ou les services proposés dans le processus de vote. Cela porte également atteinte au droit de vote. Si le bulletin de vote est généré à partir d'une liste électorale falsifiée ou modifiée, le suffrage exprimé et la

1. Par exemple, une réglementation interdisant de publier des listes électorales pour protéger la vie privée

décision de l'électeur sont affectés, car un bulletin de vote falsifié est généré. Un dysfonctionnement empêche le suffrage d'entrer dans l'urne électronique sans que l'électeur en soit conscient ou averti.
Subtilité : la menace existe si une liste des candidats ou d'options est nécessaire pendant la période du scrutin, par exemple pour générer le bulletin de vote.
Note pour la mise en œuvre : la liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme atteste le droit de vote.
N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter l'expression de suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire.

T.Vote_Confidentiality – *Confidentialité de la décision de l'électeur*

Un agresseur prend connaissance d'un vote. Un agresseur découvre l'identité de l'électeur par le biais du vote.

T.Vote_DOS – *Attaque par saturation contre le processus de vote*

L'agresseur interrompt le processus de vote ou les services, donc la disponibilité du processus pendant la période des élections n'est pas assurée.
L'agresseur empêche un électeur d'exprimer son suffrage à l'aide du système de vote électronique, ce qui porte atteinte au droit de vote de l'électeur. Les attaques par déni de service ou par saturation du système retardent le transfert du suffrage et l'empêchent d'accéder à l'urne électronique avant la clôture de la période du scrutin.

T.Vote_Modify – *Disponibilité et intégrité des suffrages exprimés*

Un agresseur modifie les suffrages, générant des suffrages qui ne correspondent pas à la décision des électeurs. Un agresseur détruit irrémédiablement des suffrages.

T.Vote_Multiple – *Usurpation de l'identité d'un électeur habilité à voter*

Un agresseur ou un électeur vote plusieurs fois via un dispositif de vote spécifique ou à l'aide de multiples dispositifs de vote. Cela porte atteinte au droit de vote qui implique également la règle du vote unique.

T.Vote_Time – *Manipulation du temps ou du délai de vote*

Un agresseur met hors service la source de synchronisation du processus de vote ou modifie la date et l'heure auxquelles une inscription est intervenue soit pour faire accepter un suffrage exprimé hors délai, soit pour disqualifier un suffrage exprimé dans les temps. Cela porte atteinte au droit de vote.

T.Vote_Trail – *Sûreté des voies suivies par l'information compromise*

Un agresseur accède aux voies suivies par l'information qui établissent un lien entre un suffrage et l'identité d'un électeur. Cela compromet la décision de l'électeur.

T.Voter_Impers – *Usurpation de l'identité d'un électeur légitime*

Un agresseur usurpe l'identité d'un électeur légitime. Cela porte atteinte au droit de vote, ainsi qu'à la décision de l'électeur et au suffrage, car ce suffrage diffère des intentions de l'électeur légitime.

T.Voter_Privacy – *Divulgation de données à caractère personnel*

Un agresseur révèle des données à caractère personnel de l'électeur.
Note pour la mise en œuvre : la législation applicable à la publication ou à la divulgation des listes électorales peut varier d'un pays à l'autre.

T.VotReg_Disclose – voir *Période préélectorale*

Note pour la mise en œuvre : la liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme atteste le droit de vote.
N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter les suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire.

T.VotReg_Modify – voir *Période préélectorale*

Note pour la mise en œuvre : la liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme atteste le droit de vote.
N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter l'expression de suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire.

Période postélectorale

T.CommD_Avail_elec – *Disponibilité/intégrité des données issues de la période du scrutin*

Un agresseur modifie ou interrompt le flux de données communiquées depuis la période du scrutin. Il en résulte une falsification ou la disparition de la liste des suffrages, ce qui fausse les résultats du scrutin et les listes de candidats, ou fait disparaître ces dernières.
Note pour la mise en œuvre : la liste d'options ou de candidats peut être nécessaire à l'élaboration des résultats ou du rapport des élections ou du référendum.

T.CommD_Sec_elec – *Confidentialité des données communiquées issues de la période du scrutin*

Un agresseur prend connaissance de suffrages communiqués.

T.Count_DOS – *Attaque par saturation contre le dépouillement*

Un agresseur interrompt le dépouillement ou ses services ; la disponibilité du résultat des élections n'est donc plus assurée.

T.Malfunction_post – *Dysfonctionnement des systèmes ou services en période postélectorale*

Un dysfonctionnement détruit irrémédiablement des suffrages, interrompt le dépouillement ou engendre, lors du dépouillement, des erreurs qui affectent le résultat du scrutin. Un dysfonctionnement perturbe la capacité de générer un rapport d'élection ou détruit irrémédiablement le rapport d'élection.

T.MisCount – *Comptage incorrect*

Un agresseur manipule le dépouillement, ce qui fausse les résultats.

T.Partial_Count – *Comptage partiel*

Un agresseur lance le comptage de sous-ensembles choisis dans les suffrages, ce qui peut révéler un suffrage (décision d'un électeur) à partir des voies suivies par l'information.

T.Premature_Count – *Comptage prématuré ou divulgation de résultats partiels*

Un agresseur lance le comptage avant l'heure prescrite et accède à des résultats partiels ou prématurés. Ces résultats partiels affectent également la confidentialité des suffrages (décisions des électeurs) à partir des voies suivies par l'information.

T.Report_DOS – *Attaque par saturation contre le processus de rapport*

Un agresseur interrompt le processus de rapport ou ses services ; la disponibilité du rapport d'élection ou de référendum n'est donc plus assurée.

T.Report_Modify – *Modification du rapport d'élection ou de référendum*

Un agresseur modifie le rapport d'élection ou de référendum.

T.Result_Modify – *Modification du résultat du scrutin*

Un agresseur modifie le résultat du scrutin.

T.Vote_Confidentiality – voir *Période du scrutin*

T.Vote_Duplicates – *Modification du résultat du scrutin*

Un agresseur ou un dysfonctionnement génère des copies des suffrages qui ne peuvent être détectées comme telles, ce qui affecte le résultat du scrutin.

T.Vote_Modify – voir *Période du scrutin*

T.Vote_Trail – voir *Période du scrutin*

Les tableaux 1 à 3 ci-après fournissent une vue d'ensemble des menaces par rapport aux avantages qu'elles affectent aux diverses étapes du processus. Les avantages et les menaces qui concernent plusieurs étapes du processus (hormis les avantages/menaces généraux) sont marqués d'un astérisque.

Tableau 1 : Avantages et menaces correspondantes en période préélectorale

	Avantages / **Menaces**	en général			période préélectorale								
		Données d'authentification	Vérifiab./Observab.	Intégrité du système	Décision de candidat	Liste des candidats *	Liste électorale *	Processus de désignation	Délai d'inscription	Vie privée *	Processus d'inscription	Délai de désignation	Droit de vote*
en général	T.Audit_Forgery		X										
	T.Auth_Disclose	X											
	T.Hack	X	X	X	X	X	X	X	X	X	X	X	X
	T.Observ_Forgery		X										
	T.System_Forgery	X	X	X	X	X	X	X	X	X	X	X	X
période préélectorale	T.CandList_Disclose				X	X				X			
	T.CandList_Modify *				X	X							
	T.Malfunction_pre					X	X	X			X		X
	T.Nomin_DOS				X	X		X					
	T.Nomin_Time				X	X			X				
	T.Privacy				X	X	X			X			
	T.Registr_DOS						X				X		X
	T.Registr_Time											X	
	T.VotReg_Disclose *						X			X			
	T.VotReg_Modify *						X						X

Tableau 2 : Avantages et menaces correspondantes en période de scrutin

Avantages / Menaces		en général			période de scrutin								
		Données d'authentification	Vérifiab./observab.	Intégrité du système	Bulletin de vote	Liste des candidats *	Liste électorale *	Droit de vote *	Vote *	Décision d'électeur *	Vie privée de l'électeur	Jour/heure d'expression d'un suffrage	Processus de vote
en général	T.Audit_Forgery		X										
	T.Auth_Disclose	X											
	T.Hack	X	X	X	X	X	X	X	X	X	X	X	X
	T.Observ_Forgery		X										
	T.System_Forgery	X	X	X	X	X	X	X	X	X	X	X	X
période de scrutin	T.Ballot_Forgery				X				X	X			
	T.CandList_Modify *				X	X			X	X			
	T.CommD_Avail_pre					X	X	X					
	T.CommD_Sec_pre						X						
	T.Malfunction_elect				X	X	X	X	X	X			X
	T.Vote_Confidentiality*								X	X			
	T.Vote_DOS							X					X
	T.Vote_Modify *								X	X			
	T.Vote_Multiple							X					
	T.Vote_Time							X				X	
	T.Vote_Trail *									X			
	T.Voter_Impers							X	X	X			
	T.Voter_Privacy					X					X		
	T.VotReg_Disclose *						X				X		
	T.VotReg_Modify *						X	X					

Tableau 3 : Avantages et menaces correspondantes en période postélectorale

	Avantages / Menaces	en général			période postélectorale					
		Données d'authentification	Vérifiab./Observab.	Intégrité du système	Liste des candidats *	Dépouillement	Résultat du scrutin	Rapport d'élection	Vote	Processus de rapport
en général	T.Audit_Forgery		X							
	T.Auth_Disclose	X								
	T.Hack	X	X	X	X	X	X	X	X	X
	T.Observ_Forgery		X							
	T.System_Forgery	X	X	X	X	X	X	X	X	X
période postélectorale	T.CommD_Avail_elec				X		X		X	
	T.CommD_Sec_elec								X	X
	T.Count_DOS					X	X			
	T.Malfunction_Post					X	X	X	X	
	T.MisCount						X			
	T.Partial_Count								X	X
	T.Premature_Count						X		X	X
	T.Report_DOS							X		
	T.Report_Modify							X		
	T.Result_Modify						X			
	T.Vote_Confidentiality*								X	X
	T.Vote_Duplicates						X		X	
	T.Vote_Modify *						X		X	
	T.Vote_Trail *								X	X

Objectifs de sécurité

Cette section relève et définit les objectifs de sécurité en matière de vote électronique. Ces objectifs correspondent à la volonté déclarée et parent aux menaces identifiées. Les objectifs de sécurité énoncés dans cette section correspondent aux impératifs de sécurité présentés dans la rubrique Sécurité de l'Annexe III.

Objectifs généraux

O.Access_Cntrl – *Contrôle d'accès*

Le système de vote doit restreindre l'accès à ses services, en fonction de l'identité de l'utilisateur ou de son rôle, aux services explicitement ouverts à cet utilisateur ou à ce rôle. L'identité de l'utilisateur doit être authentifiée avant toute action.

O.Assessment – *Evaluation indépendante*

Le respect de ces recommandations devra être vérifié par des organismes indépendants.
Note pour la mise en œuvre : si des profils de protection CC/Iso 15408 évalués et certifiés sont élaborés sur la base de cette recommandation de sécurité, une évaluation indépendante est réalisée dans le cadre du programme des CC.

O.Auth_User – *Authentification de l'identité des utilisateurs*

Le système de vote ou ses éléments doivent protéger les données d'authentification de manière à empêcher des entités non autorisées de détourner, d'intercepter, de modifier ou de prendre connaissance à toute autre fin de tout ou partie des données d'authentification. Il est recommandé de recourir à une authentification fondée sur la cryptographie.
Note pour la mise en œuvre : cet objectif concerne tous les sujets. Les services informant, par exemple, les électeurs avant leur entrée dans le processus de vote (pour lesquels l'authentification est évidemment sans objet) ne sont pas concernés par ce document.

O.Avail – *Disponibilité des processus de l'élection électronique*

Des mesures techniques et organisationnelles doivent être prises pour garantir qu'aucune donnée ne soit définitivement perdue en cas de panne ou de problèmes affectant le système de vote électronique. Le système d'élection électronique doit préserver la disponibilité de ses services durant le processus de vote électronique. Il doit notamment résister aux dysfonctionnements, aux pannes ou aux attaques par saturation.
Note pour la mise en œuvre : des contrats de niveau de service définissent en général la disponibilité et la fréquence des pannes. Un certain niveau de dégradation de service peut être admissible pendant les périodes de dérangement, par exemple quand un serveur d'un réseau 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 devra toutefois le tester à l'aide d'attaques délibérées par saturation et documenter les réserves de moyens prévues pour maintenir le fonctionnement du système. Des tests indépendants d'intrusion peuvent diminuer les chances de succès des attaques par saturation.
Subtilité : les services dont la disponibilité doit être préservée dépendent de la période concernée (préélectorale, de scrutin ou postélectorale). En période préélectorale, les processus de désignation et d'inscription et les services correspondants doivent être disponibles ; en période de scrutin, ce sont les processus de vote et les services correspondants ; et en période postélectorale ce sont les processus de dépouillement et de communication des résultats et les services correspondants. Les processus de vérification doivent être opérationnels à toutes les étapes. Les limites prédéfinies des contrats de niveau de service, les taux de pannes acceptables ou les dégradations de service peuvent toutefois varier suivant les différents stades ou services.

O.Ident_User – *Authentification de l'identité des utilisateurs fondée sur l'identité*

L'identification spécifique des électeurs et des candidats doit être assurée.
Note pour la mise en œuvre : l'authentification peut se fonder sur l'identité ou sur le rôle. Celle fondée sur l'identité est recommandable pour l'inscription des électeurs ou l'expression des suffrages, ou pour l'acceptation ou le rejet d'une désignation ; mais l'authentification fondée sur le rôle suffit sans doute pour les administrateurs, les vérificateurs, etc.

O.Observation_Data – *Données d'observation*

Le système de vote électronique doit générer des données d'observation fiables et assez détaillées pour autoriser le bon déroulement de l'observation des élections. Il doit être possible de déterminer avec certitude la date et l'heure à laquelle un événement a généré des données d'observation. L'authenticité, la disponibilité et l'intégrité des données doivent être assurées.

O.Privacy – *Vie privée des électeurs et des candidats*

Le système de vote doit préserver la vie privée des personnes. La confidentialité des listes électorales enregistrées ou communiquées par le système de vote doit être assurée.
Subtilité : quand elles sont stockées ou communiquées dans un environnement non contrôlé, les listes électorales doivent être cryptées.
Note pour la mise en œuvre : suivant les pratiques nationales, des exigences de confidentialité supplémentaires peuvent entourer les décisions des candidats. La confidentialité est alors de mise.

O.Reliable_Time – *Source de synchronisation fiable*

Le système de vote doit assurer une source de synchronisation fiable. La précision de la source de synchronisation devra être suffisante pour gérer les repères temporels des voies suivies par l'information d'audit et des données d'observation, ainsi que les délais d'inscription, de désignation, de vote ou de dépouillement. Note pour la mise en œuvre : la précision nécessaire peut varier suivant les utilisateurs de la source de synchronisation, selon les tolérances appliquées par exemple à l'inscription et à l'expression des suffrages. L'on peut donc envisager 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 capitaux, tandis que des séquences continues de chiffres ou la préservation de la séquence pourraient suffire dans les entrées de journal. Notons toutefois que l'exactitude des repères temporels peut compromettre la confidentialité du choix des électeurs.

O.Secure_Oper – *Sécurité d'exploitation et intégrité du système*

Le système de vote électronique vérifiera à intervalles réguliers que le fonctionnement est conforme aux spécifications techniques de ses éléments et que ses services sont disponibles.

Période préélectorale

O.Data_Sec – *Disponibilité et intégrité de l'élection ou du référendum, des options, de la liste des candidats*

Les listes électorales et les listes des candidats doivent être préservées des points de vue de leur authenticité, de leur disponibilité et de leur intégrité. L'origine des données doit être authentifiée. Les dispositions relatives à la protection des données doivent être prises en compte.
Subtilité : la législation en matière de confidentialité ou de publication des décisions de candidats ou de la liste électorale peut varier d'un pays à l'autre.
Note pour la mise en œuvre : l'authentification de l'origine des données peut, par exemple, être assurée par des signatures électroniques dans les processus entièrement informatisés. Quand l'informatisation n'est que partielle, l'authentification de l'origine des données peut aussi faire appel à des mesures de sécurité conventionnelles telles que les signatures manuelles, les cachets, les courriers, etc.

O.Time_Nominate – *Désignation dans les temps*

Le fait que la désignation d'un candidat et la décision de ce dernier et/ou celle de l'autorité électorale compétente de l'accepter sont intervenues dans les délais prescrits sera vérifiable.

Note pour la mise en œuvre : cela peut, par exemple, être assuré par horodatage ou par la confirmation d'un système fiable.

O.Time_Register – *Inscription dans les temps*

Le fait que l'inscription a été effectuée dans les délais prescrits doit être vérifiable.
Note pour la mise en œuvre : cela peut, par exemple, être assuré par horodatage ou par la confirmation d'un système fiable.

Période du scrutin

O.Authentic_Vote – *Assurer l'authenticité du scrutin*

Le système de vote électronique doit garantir à l'électeur que son choix sera parfaitement représenté dans l'élection et que son bulletin entrera scellé dans l'urne électronique.

O.Ballot_Correct – *Présentation d'un bulletin de vote correct*

Il faudra garantir que le système de vote électronique présente un bulletin de vote authentique à l'électeur. En cas de vote électronique à distance, l'électeur sera informé des moyens permettant de vérifier qu'il est bien connecté au serveur officiel et que le bulletin authentique lui est présenté.
Note pour la mise en œuvre : un attaquant peut présenter de faux systèmes, en imitant un serveur officiel par manipulation du système de nom de domaine (DNS), en utilisant un nom de domaine similaire à celui du serveur officiel, en usurpant l'identité du client et du serveur (attaque de type *man-in-the-middle*) ou par un cheval de Troie dans le système de l'électeur, qui remplace le bulletin original ou injecte de faux bulletins. Une signature électronique appliquée par les autorités électorales sur le bulletin permet de vérifier ce dernier. Cela ne doit toutefois pas engendrer une violation du secret de la décision de l'électeur. En d'autres termes, les données établissant qu'un bulletin est correct ne doivent pas rendre les bulletins identifiables, à moins que ces données spécifiques soient supprimées quand l'électeur exprime son suffrage.

O.Delayed_Vote – *Accepter un suffrage exprimé hors délai*

A l'expiration de la période du scrutin, aucun électeur ne pourra accéder au système de vote électronique. Il convient toutefois que le système accepte les suffrages dans l'urne électronique pendant un temps suffisant pour prendre en compte tout retard que pourraient prendre les messages dans leur cheminement électronique.
Note pour la mise en œuvre : dans les votes à distance, les services peuvent s'attendre à une charge plus importante peu avant la fermeture du scrutin. Cette surcharge peut se traduire par des temps de transfert plus longs des suffrages exprimés vers les urnes électroniques. Les suffrages exprimés à temps doivent

être acceptés. Il convient donc que les serveurs ne se ferment pas immédiatement à l'expiration du délai si des retards de ce genre sont prévisibles.

O.Sec_Transfer_pre – *Sûreté du transfert des données communiquées*

L'intégrité des données communiquées à partir de la période préélectorale (liste des candidats, liste électorale, suivant ce qui est nécessaire pendant la période du scrutin) doit être assurée. Le système doit procéder à une authentification de l'origine des données.
Subtilité : les listes des candidats et d'options sont nécessaires pendant la période du scrutin si le bulletin de vote est généré pendant cette période.
Subtilité : la liste électorale peut être superflue si, dans une élection à deux tours, un jeton anonyme atteste le droit de vote.
N.B. Les listes électorales peuvent s'avérer nécessaires dans les bureaux de vote pour éviter les suffrages multiples (électroniques et sur papier) ou en cas de vote obligatoire.
Note pour la mise en œuvre : l'authentification de l'origine des données peut, par exemple, être assurée par des signatures électroniques dans les processus entièrement informatisés. Quand l'informatisation n'est que partielle, l'authentification de l'origine des données peut aussi faire appel à des mesures de sécurité conventionnelles telles que les signatures manuelles, les cachets, les courriers, etc.

O.System_Secure – *Sûreté du système de vote*

Des moyens suffisants doivent être mis en œuvre pour protéger les systèmes qu'utilisent les électeurs pour exprimer leur suffrage contre les influences visant à modifier leur décision.
Subtilité : dans le cas d'un cadre non surveillé de vote à distance, comme le vote par l'Internet, l'électeur ou des tiers contrôlent généralement l'environnement. Le système de vote peut difficilement contrôler l'existence d'un environnement sécurisé. Il faudra prévoir des moyens d'augmenter la confiance des utilisateurs dans les systèmes, par exemple la possibilité de vérifier qu'ils sont en présence du logiciel authentique, ou des recommandations indiquant comment protéger l'environnement du système.

O.Residual_Info – *Détruire les informations résiduelles*

Les informations résiduelles qui renferment la décision de l'électeur, ou l'image d'écran où s'affiche son choix, doivent être détruites dès que le suffrage est exprimé. En cas de vote électronique à distance, il conviendra de fournir à l'électeur, si cette possibilité existe, des informations sur la marche à suivre pour effacer de telles données de l'appareil utilisé pour enregistrer son suffrage.
Note pour la mise en œuvre : le cache des navigateurs Internet, les données passant par les disques durs, les fichiers temporaires, etc. peuvent contenir des

informations résiduelles. Il existe diverses parades, telles que la conception d'applications Internet évitant de générer certains types d'informations résiduelles. L'efficacité de telles mesures dépend toutefois de l'application utilisée par l'électeur et de sa configuration. Dans le cadre non surveillé d'un vote à distance, comme le vote par l'Internet, l'électeur ou des tiers contrôlent généralement l'environnement. Le système de vote peut difficilement vérifier la présence d'un environnement sécurisé. Il faut offrir des moyens d'augmenter la confiance des utilisateurs dans le système, par exemple leur permettre de s'assurer qu'ils sont en présence du véritable logiciel ou leur donner des recommandations indiquant comment protéger l'environnement du système.

O.Time_Vote – *Expression du suffrage dans les délais*

Le fait que le suffrage ait été exprimé dans les délais prescrits doit être vérifiable. Note pour la mise en œuvre : cela peut, par exemple, être assuré par horodatage ou par la confirmation d'un système fiable. Les informations d'horodatage ne doivent toutefois pas générer des voies suivies par l'information susceptibles de révéler la décision de l'électeur (voir O.Vote_Confidentiality).

O.Vote_Confidentiality – *Anonymat de l'électeur*

Les bulletins et les informations concernant les électeurs doivent rester sous scellés aussi longtemps que les données qu'ils contiennent peuvent être recoupées. Les informations permettant d'identifier l'électeur doivent être séparées de son bulletin de vote à une étape prédéfinie dans l'élection ou le référendum électroniques.
N.B. Cet objectif implique des exigences techniques. Il est toutefois aussi repris dans les normes juridiques sous « Fiabilité et sécurité », norme n° 35.

O.Vote_Secure – *Disponibilité, confidentialité et intégrité des suffrages exprimés*

Le système de vote électronique doit assurer la disponibilité et l'intégrité des suffrages pendant toute sa durée de vie. Le système de vote électronique doit préserver la confidentialité des suffrages et les maintenir scellés jusqu'au dépouillement. S'ils sont stockés ou communiqués dans un environnement non contrôlé, les suffrages doivent être cryptés.
N.B. Cet objectif implique des exigences techniques. Il est toutefois aussi repris dans les normes juridiques sous « Fiabilité et sécurité », norme n° 34.
Note pour la mise en œuvre : le cryptage est une excellente technique de protection de la confidentialité des suffrages, surtout dans un vote à distance où les suffrages exprimés sont transmis via des lignes publiques. S'il s'agit de machines de vote dans des bureaux de vote, une protection matérielle peut aussi servir cette fin. La définition du scellement (donnée dans la recommandation) établit une distinction entre le cryptage et les circuits fermés, par exemple. Dans les environnements non contrôlés, les mesures de sécurité les plus performantes sont exigées pour protéger les suffrages, qui sont le premier avantage retiré des

élections électroniques, ainsi que la confidentialité de la décision des électeurs, qui est vraisemblablement leur préoccupation première. Cette exigence appelle donc explicitement un cryptage.

O.Voter_Eligible – *Authentification d'un électeur habilité à exprimer un suffrage*

Le système d'élection électronique doit vérifier qu'un électeur qui tente de voter est habilité à le faire. Le système d'élection électronique doit être capable d'authentifier l'identité de l'électeur et de garantir que seul le nombre de suffrages autorisé par électeur est stocké dans l'urne électronique.
Subtilité : quand des jetons anonymes de vote attestent le droit de vote d'un électeur, l'authentification de l'électeur peut être facultative. Il faut cependant encore l'empêcher d'exprimer des suffrages multiples dans l'anonymat.

Période postélectorale

O.Count_Correct – *Exactitude et reproductibilité du résultat du dépouillement*

Le processus de dépouillement dénombrera les suffrages avec précision. Le résultat du scrutin doit être reproductible.

O.Result_Secure – *Disponibilité et intégrité de l'urne et du résultat*

Le système d'élection électronique doit assurer la disponibilité et l'intégrité del'urne électronique et du résultat du dépouillement aussi longtemps que nécessaire.

O.Sec_Transfer_vote – *Sécurité du transfert des données communiquées*

L'intégrité des données communiquées depuis la période du scrutin (exemple : suffrages, liste d'électeurs, liste des candidats) sera préservée. L'origine des données sera authentifiée.
Note pour la mise en œuvre : l'authentification de l'origine des données peut, par exemple, être assurée par des signatures électroniques dans les processus entièrement informatisés. Quand l'informatisation n'est que partielle, l'authentification de l'origine des données peut aussi faire appel à des mesures de sécurité conventionnelles comme les signatures manuelles, les cachets, les courriers, etc. Les suffrages exprimés ou les résultats partiels du dépouillement sont les avantages les plus précieux d'un scrutin. Il est donc préférable de prendre les mesures techniques qui s'imposent pour protéger ces avantages pendant le transfert.

O.Vote_Confidentiality – voir *Période du scrutin.*

O.Vote_Secure – voir *Période du scrutin.*

Les tableaux 4 à 7 ci-après mettent les objectifs en regard des menaces contrées. Les menaces qui figurent dans plusieurs étapes du processus (hormis les avantages/menaces généraux) sont marquées d'un astérisque.

Tableau 4 : Synoptique des objectifs par rapport aux menaces, objectifs généraux pour toutes les périodes

	Objectifs généraux / Menaces	O.Access_Cntrl	O.Assessment	O.Auth_User	O. Avail	O.Ident_User	O.Observation_Data	O.Privacy	O.Reliable_Time	O.Secure_Oper
en général	T.Audit_Forgery	X	La garantie ne contre pas directement les menaces, mais elle rassure sur le bon fonctionnement, sur le fait que les menaces sont indirectement contrées	X					X	
	T.Auth_Disclose	X		X						
	T.Hack	X		X	X					X
	T.Observ_Forgery	X		X			X		X	
	T.System_Forgery	X		X			X			X
période préélectorale	T.CandList_Disclose	X		X			L'observation contribue au bon fonctionnement du scrutin, et pare donc indirectement les menaces	X		
	T.CandList_Modify *	X		X	X					
	T.Malfunction_pre				X					X
	T.Nomin_DOS				X					X
	T.Nomin_Time	X		X					X	
	T.Privacy	X		X		X		X		
	T.Registr_DOS				X					X
	T.Registr_Time	X		X					X	
	T.VotReg_Disclose *	X		X				X		
	T.VotReg_Modify *	X		X	X	X				
période de scrutin	T.Ballot_Forgery									X
	T.CandList_Modify *	X		X						
	T.CommD_Avail_pre	X		X	X					
	T.CommD_Sec_pre	X		X				X		
	T.Malfunction_elect				X					X
	T.Vote_Confidentiality*									
	T.Vote_DOS				X					X
	T.Vote_Modify *	X		X						
	T.Vote_Multiple					X				
	T.Vote_Time	X		X					X	
	T.Vote_Trail *									
	T.Voter_Impers	X		X		X				
	T.Voter_Privacy	X		X				X		
	T.VotReg_Disclose *	X		X				X		
	T.VotReg_Modify *	X		X						

période postélectorale	T.CommD_Avail_elec	X		X						
	T.CommD_Sec_elec	X		X						
	T.Count_DOS				X					X
	T.Malfunction_Post				X					X
	T.MisCount									
	T.Partial_Count	X		X						
	T.Premature_Count	X		X					X	
	T.Report_DOS				X					X
	T.Report_Modify	X		X						
	T.Result_Modify	X		X						
	T.Vote_Confidentiality*									
	T.Vote_Duplicates									
	T.Vote_Modify *	X		X						
	T.Vote_Trail *									

Tableau 5 : Synoptique des objectifs par rapport aux menaces en période préélectorale

Objectifs / Menaces		en général	période préélectorale		
			O.Data_Sec *	O.Time_Nominate	O.Time_Register
en général	T.Audit_Forgery	voir tableau 4			
	T.Auth_Disclose				
	T.Hack				
	T.Observ_Forgery				
	T.System_Forgery				
période préélectorale	T.CandList_Disclose	voir tableau 4	X		
	T.CandList_Modify*		X		X
	T.Malfunction_pre				
	T.Nomin_DOS				
	T.Nomin_Time			X	
	T.Privacy		X		
	T.Registr_DOS				
	T.Registr_Time				X
	T.VotReg_Disclose *		X		
	T.VotReg_Modify*		X	X	

Tableau 6 : Synoptique des objectifs par rapport aux menaces en période du scrutin

	Objectifs / Menaces	En général	période de scrutin										
			O.Ballot_Correct	O.Correct_Vote	O.Delayed_Vote *	O.Feedback *	O.Sec_Transfer_pre	O.System_Secure	O.Residual	O.Time_Vote	O.Vote_Secure	O.Vote_Secrecy	O.Voter_Eligible
en général	T.Audit_Forgery	voir tableau 4											
	T.Auth_Disclose							X					
	T.Hack					X		X					
	T.Observ_Forgery												
	T.System_Forgery							X					
période de scrutin	T.Ballot_Forgery	voir tableau 4	X	X			X	X					
	T.CandList_Modify *						X						
	T.CommD_Avail_pre						X						
	T.CommD_Sec_pre						X						
	T.Malfunction_elect			X		X		X					
	T.Vote_Confidentiality*			X				X	X		X	X	
	T.Vote_DOS			X	X	X				X			
	T.Vote_Modify *		X	X				X		X	X		
	T.Vote_Multiple												X
	T.Vote_Time									X			
	T.Vote_Trail *								X	X		X	
	T.Voter_Impers							X					X
	T.Voter_Privacy										X	X	
	T.VotReg_Disclose *						X						
	T.VotReg_Modify *		X	X			X						

Tableau 7 : Synoptique des objectifs par rapport aux menaces en période post-électorale

Objectifs / Menaces		en général	période postélectorale				
			O.Count_Correct	O.Result_Secure	O.Sec_Transfer_vote	O.Vote_Secure	O.Vote_Confidentiality
en général	T.Audit_Forgery	voir tableau 4					
	T.Auth_Disclose						
	T.Hack						
	T.Observ_Forgery						
	T.System_Forgery						
période postélectorale	T.CommD_Avail_elec	voir tableau 4			X		
	T.CommD_Sec_elec				X		
	T.Count_DOS						
	T.Malfunction_Post						
	T.MisCount		X				
	T.Partial_Count			X			X
	T.Premature_Count						
	T.Report_DOS						
	T.Report_Modify				X		
	T.Result_Modify			X	X		
	T.Vote_Confidentiality*					X	X
	T.Vote_Duplicates		X				
	T.Vote_Modify *					X	
	T.Vote_Trail *						X

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

BELGIUM/BELGIQUE
La Librairie européenne SA
50, avenue A. Jonnart
B-1200 BRUXELLES 20
Tel.: (32) 2 734 0281
Fax: (32) 2 735 0860
E-mail: info@libeurop.be
http://www.libeurop.be

Jean de Lannoy
202, avenue du Roi
B-1190 BRUXELLES
Tel.: (32) 2 538 4308
Fax: (32) 2 538 0841
E-mail: jean.de.lannoy@euronet.be
http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Company Limited
5369 Chemin Canotek Road
CDN-OTTAWA, Ontario, K1J 9J3
Tel.: (1) 613 745 2665
Fax: (1) 613 745 7660
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

CZECH REPUBLIC/
RÉPUBLIQUE TCHÈQUE
Suweco Cz Dovoz Tisku Praha
Ceskomoravska 21
CZ-18021 PRAHA 9
Tel.: (420) 2 660 35 364
Fax: (420) 2 683 30 42
E-mail: import@suweco.cz

DENMARK/DANEMARK
GAD Direct
Fiolstaede 31-33
DK-1171 COPENHAGEN K
Tel.: (45) 33 13 72 33
Fax: (45) 33 12 54 94
E-mail: info@gaddirect.dk

FINLAND/FINLANDE
Akateeminen Kirjakauppa
Keskuskatu 1, PO Box 218
FIN-00381 HELSINKI
Tel.: (358) 9 121 41
Fax: (358) 9 121 4450
E-mail: akatilaus@stockmann.fi
http://www.akatilaus.akateeminen.com

FRANCE
La Documentation française
(Diffusion/Vente France entière)
124, rue H. Barbusse
F-93308 AUBERVILLIERS Cedex
Tel.: (33) 01 40 15 70 00
Fax: (33) 01 40 15 68 00
E-mail: commandes.vel@ladocfrancaise.gouv.fr
http://www.ladocfrancaise.gouv.fr

Librairie Kléber (Vente Strasbourg)
Palais de l'Europe
F-67075 STRASBOURG Cedex
Fax: (33) 03 88 52 91 21
E-mail: librairie.kleber@coe.int

GERMANY/ALLEMAGNE
AUSTRIA/AUTRICHE
UNO Verlag
August Bebel Allee 6
D-53175 BONN
Tel.: (49) 2 28 94 90 20
Fax: (49) 2 28 94 90 222
E-mail: bestellung@uno-verlag.de
http://www.uno-verlag.de

GREECE/GRÈCE
Librairie Kauffmann
28, rue Stadiou
GR-ATHINAI 10564
Tel.: (30) 1 32 22 160
Fax: (30) 1 32 30 320
E-mail: ord@otenet.gr

HUNGARY/HONGRIE
Euro Info Service
Hungexpo Europa Kozpont ter 1
H-1101 BUDAPEST
Tel.: (361) 264 8270
Fax: (361) 264 8271
E-mail: euroinfo@euroinfo.hu
http://www.euroinfo.hu

ITALY/ITALIE
Libreria Commissionaria Sansoni
Via Duca di Calabria 1/1, CP 552
I-50125 FIRENZE
Tel.: (39) 556 4831
Fax: (39) 556 41257
E-mail: licosa@licosa.com
http://www.licosa.com

NETHERLANDS/PAYS-BAS
De Lindeboom Internationale Publikaties
PO Box 202, MA de Ruyterstraat 20 A
NL-7480 AE HAAKSBERGEN
Tel.: (31) 53 574 0004
Fax: (31) 53 572 9296
E-mail: books@delindeboom.com
http://home-1-worldonline.nl/~lindeboo/

NORWAY/NORVÈGE
Akademika, A/S Universitetsbokhandel
PO Box 84, Blindern
N-0314 OSLO
Tel.: (47) 22 85 30 30
Fax: (47) 23 12 24 20

POLAND/POLOGNE
Główna Księgarnia Naukowa
im. B. Prusa
Krakowskie Przedmiescie 7
PL-00-068 WARSZAWA
Tel.: (48) 29 22 66
Fax: (48) 22 26 64 49
E-mail: inter@internews.com.pl
http://www.internews.com.pl

PORTUGAL
Livraria Portugal
Rua do Carmo, 70
P-1200 LISBOA
Tel.: (351) 13 47 49 82
Fax: (351) 13 47 02 64
E-mail: liv.portugal@mail.telepac.pt

SPAIN/ESPAGNE
Mundi-Prensa Libros SA
Castelló 37
E-28001 MADRID
Tel.: (34) 914 36 37 00
Fax: (34) 915 75 39 98
E-mail: libreria@mundiprensa.es
http://www.mundiprensa.com

SWITZERLAND/SUISSE
Adeco – Van Diermen
Chemin du Lacuez 41
CH-1807 BLONAY
Tel.: (41) 21 943 26 73
Fax: (41) 21 943 36 05
E-mail: info@adeco.org

UNITED KINGDOM/ROYAUME-UNI
TSO (formerly HMSO)
51 Nine Elms Lane
GB-LONDON SW8 5DR
Tel.: (44) 207 873 8372
Fax: (44) 207 873 8200
E-mail: customer.services@theso.co.uk
http://www.the-stationery-office.co.uk
http://www.itsofficial.net

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Company
2036 Albany Post Road
CROTON-ON-HUDSON,
NY 10520, USA
Tel.: (1) 914 271 5194
Fax: (1) 914 271 5856
E-mail: Info@manhattanpublishing.com
http://www.manhattanpublishing.com

Council of Europe Publishing/Editions du Conseil de l'Europe
F-67075 Strasbourg Cedex
Tel.: (33) 03 88 41 25 81 – Fax: (33) 03 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int