### 2.2.3. Variante "PROVEN" [L3]

**Le concept global de sécurité du vote électronique fait l'objet d'une évaluation publique préalable et est accepté par la grande majorité des cyber-experts. Les cantons reçoivent des conditions concrètes. Les tests actuels sont suspendus jusqu'à la mise en œuvre.**

[1)]La Confédération peut édicter des restrictions à l'utilisation du vote électronique.

[2)]La Confédération présente dans un délai de [18 mois] un **concept de sécurité global** pour l'introduction régulière du vote électronique, dans lequel au moins [90%] des experts en cybersécurité ***impliqués et intéressés*** attestent de l'efficacité des mesures prises en vue d'une fiabilité absolue du résultat des élections.

[3)]Les cantons se voient imposer des obligations en matière de surveillance, de contrôle et de suivi médico-légal en cas d'irrégularités par le service central fédéral "Cyber Defence".

[4)]Ces mesures de sécurité comprennent notamment la garantie de la traçabilité de toutes les interventions dans le système de vote électronique (y compris les plateformes), des contrôles de sécurité des personnes, des mesures contre l'ingénierie sociale, une gestion des incidents, l'exploitation et la sécurité des centres d'impression qui délivrent les codes et la mise en place d'un centre de services pour les besoins de la sécurité des terminaux des utilisateurs.

[5)]Les compétences et l'étendue des tâches mentionnées sont rendues publiques. Les organismes sont tenus d'apporter la preuve de leur mise en œuvre. Toutes les irrégularités et les mesures prises pour y remédier doivent être publiées à chaque fois.

[6)]Le concept contient également les critères sur l'annulation ou le retrait de l'élection ou du vote en cas d'apparition d'irrégularités et de résultats d'enquêtes médico-légales, ainsi que le retard éventuel de la reconnaissance dû à de telles activités.

[7)]Le test actuel est suspendu et ne reprendra qu'APRÈS la mise en œuvre des mesures conçues.

[8)]L'introduction régulière du vote électronique aura lieu une fois que le nouveau mode de test sera établi et que les ressources postulées seront disponibles et opérationnelles avec succès.

[9)]Les mesures sont examinées périodiquement par un comité d'experts et, si nécessaire, renforcées. Le comité d'experts comprend obligatoirement des cyberspécialistes indépendants.

[10)] Un calcul des coûts complets d'exploitation du vote électronique doit être établi et publié.

[11)]Si aucun document contenant les conditions mentionnées ne peut être mis à disposition dans le délai mentionné, le projet de vote électronique sera abandonné. Dans l'affirmative, le vote électronique doit être approuvé sous cette forme par référendum.

| Avantages | Inconvénients |
|---|---|
| La confiance entre les professionnels peut le plus facilement être établie si tous les points faibles et les contre-mesures sont discutés ouvertement.<br><br>Il est possible que cela permette également de stabiliser les rapports de majorité au sein du peuple et du parlement en ce qui concerne l'acceptation ou le rejet du vote électronique. | En cas de divulgation de toutes les vulnérabilités et contre-mesures, le risque d'attaques réussies augmente.<br><br>La POSTE et les cantons demanderont des fonds supplémentaires considérables à la Confédération.<br><br>Une solution acceptable sera très longue et très coûteuse. Le manque de ressources menace.<br><br>Les cantons perdent leur autonomie.<br><br>La transparence des opérations peut aussi ébranler la confiance. |

**Concevoir et mettre en œuvre la sécurité d'abord, l'introduire ensuite** !