N°	Principe	Critère	Bases dans le droit suisse
1.	Une et une seule voix pour tout citoyen ayant le droit de vote (universalité et unicité).	→**justesse**	Universalité : CF art.136 al.2 part. LDP art.8a al.2 part., ODP art. 27d al.1a & 1b Unicité : ODP art.27f al.4, ODP art. 27j
2.	L'anonymat du votant et la confidentialité de son bulletin sont garantis inconditionnellement.	→**secret**	Anonymat : ODP art 27f al.1 & 2, ODP art.27g al.1 & 4, ODP art.27h al.2 Confidentialité : LDP art.5 al.7, (anticipé:LDP art.7 al.4, correspondance:LDP art.8 al.1), LDP art.8a al.2, ODP art.27d al.1d, ODP art.27f al.3, ODP art.27g al.1
3.	Le bulletin doit contenir l'expression indubitable de la volonté (motivation) du votant.	→**conformité**	CF art.34 al.2, ODP art. 27e al.7, ATF 121 I 187
4.	Le votant de ne doit pas pouvoir voter par procuration, ni obtenir une preuve lui permettant de vendre son vote.	→**incessibilité**	Non procuration : ODP art.27a al.4 Non vente : ODP art.27h al.4 sec.part. (assimilé)
5.	Le contenu du bulletin ne peut être connu (par l'autorité qui dépouille) avant la clôture du scrutin.	→**temporalité**	ODP art.27f al.5, ODP art.27m al.2 (inverse)
6.	L'urne (ce qui en tient lieu) doit contenir tous les bulletins recueillis et eux seulement (exhaustivité et fidélité).	→**exactitude**	Fidélité : ..., CF art.34 al.2[note] Exhaustivité : LDP art.8a al.2 part., ODP art. 27d al.1e, (Préservation : ODP art.27k)
7.	Les bulletins doivent pouvoir être recomptés sensément (vérifiabilité de leur authenticité et de leur intégrité).	→**recomptabilité**	ATF 114 Ia 42[note], ATF 131 I 442, ODP art. 27n
8.	Les réclamations (avant clôture) et contestations (après) doivent pouvoir faire l'objet d'une décision dépourvue d'ambiguïté.	→**prouvabilité**	ODP art. 27n[bis]
9.	L'ensemble du processus du scrutin, la session ainsi que chaque vote, doit pouvoir être surveillé efficacement. (Les citoyens doivent pouvoir vérifier, ou faire vérifier par des personnes de confiance pour eux, la régularité du	→**transparence**	Doctrine … note1 note2

	processus)		
10.	Toute tentative de fraude est empêchée, ou détectée sans délai.	→**sécurité**	ODP art. 27d al.1c & al.1f

Note : CF = Constitution Fédérale, LDP = Loi fédérale sur les Droits Politiques, ODP = Ordonnance sur les Droits Politiques (état 1 janvier 2008); ATF = Arrêt du Tribunal Fédéral.

Par ailleurs, il est aussi attendu d'un système de vote qu'il soit ergonomique, qu'il soit fiable (résistant aux pannes, tant du côté serveur -continuité en mode dégradés, reprises sans pertes- qu'aussi du côté du votant -poursuite sans recommencement après toute interruption), qu'il soit économique (y compris offrir un débit confortable), et qu'il soit techniquement de qualité (architecture élégante, outils puissants, code solide, définitions de données sémantiquement riches) pour permettre une exploitation et une maintenance optimale.

Pour répondre au critère (1) - justesse :

Le votant doit s'identifier de manière relativement forte, et une base de données centrale (registre des électeurs) doit contrôler son droit et enregistrer en direct son mode de vote (entrée pour le local, bulletin clos reçu pour la correspondance, habilitation délivrée pour internet -voir aussi 8 prouvabilité pour la bonne fin effective).

↑critères

Pour répondre au critère (2) - secret :

Il faut garantir *inconditionnellement* la confidentialité et l'anonymat.

Pour garantir la confidentialité, le bulletin doit être rempli, confirmé et chiffré (clef de l'urne, voir 5-temporalité) localement sur le poste du votant, sans pouvoir être transporté en clair à distance (ni laisser de traces localement, voir 10-sécurité).

De plus, pour garantir l'anonymat, l'obtention du droit de vote -habilitation- et de ses instruments (bulletin vierge, etc.) doit être fait dans une autre session logique que le dépôt du bulletin, en outre l'adresse IP de l'expéditeur du bulletin doit être différente[1] de celle de la requête du droit de vote, et l'ordre d'arrivée des bulletins doit être distinct de celui des requêtes d'habilitation initiales, enfin la marque de droit de vote authentifiant le bulletin déposé (voir 7-recomptabilité) ne doit pas pouvoir être reliée à la requête de celle.ci.

↑critères

Pour répondre au critère (3) - conformité :

L'expression du choix doit être compréhensible, et sa transcription de traitement et stockage inambigüe et inaltérable.

En particulier, la motivation que le votant a exprimée, puis vérifiée et confirmée, doit être maintenue explicite et intacte au cours du transport, de l'insertion dans l'urne, du stockage,

1 Pour que l'adresse numérique internet (IP) de l'ordinateur servant au vote soit différente, il doit être possible de s'interrompre et de reprendre -sans recommencer le processus- depuis un autre poste, ou encore d'utiliser un surréseau d'intraçabilité pour délivrer le bulletin (une chaîne d'intermédiaires cloisonnés).

et ce jusqu'au dépouillement inclus (sp. jusqu'à la fin de la période de recours).

Cela se fait par un verrouillage -c.-à-d. blocage cryptographique- du texte littéral du bulletin rempli, qui a lieu entre l'expression et la confirmation, puis de la préservation de ce verrou au travers de l'envoi (chiffrement) et des opérations subséquentes (voir 7-recomptabilité, et partiellement 8-prouvabilité).

↑critères

Pour répondre au critère (4) - incessibilité :

Pour la non-procuration, le citoyen doit individuellement signer numériquement la carte de vote dématérialisée.

Pour l'invendabilité, le votant obtient bien un récépissé lui prouvant personnellement le dépôt de son bulletin dans l'urne; mais ce récépissé n'est pas probant devant un tiers, car le votant peut -mais seul lui- avoir construit un autre contenu de bulletin validant aussi le récépissé.

↑critères

Pour répondre au critère (5) - temporalité :

Le bulletin doit être crypté -sur le poste du votant et avant de le quitter- sous une clef de chiffrement asymétrique, dont la clef duale de déchiffrement (d"ouverture" de l'urne) n'est pas disponible avant la clôture du scrutin.

Pour se faire, la clef de déchiffrement doit être dispersée -à sa création, sans fuites- entre l'administration et les diverses factions politiques de la commission électorale (scrutateurs) et n'être reconstructible qu'avec la recombinaison suffisante des parties.

↑critères

Pour répondre au critère (6) - exactitude :

Pour être certain qu'il n'y a eu ni "bourrage" de l'urne (fidélité), ni soustraction de bulletins valables (exhaustivité), chaque bulletin doit être authentifié (voir 7-recomptabilité) pour garantir provenir d'un votant habilité, et les bulletins reçus doivent être chaînés de manière infalsifiable (double autorité et notarisation) pour empêcher toute suppression ultérieure.

↑critères

Pour répondre au critère (7) - recomptabilité ;

Chaque bulletin porte le texte littéral de son contenu et de la motivation du votant, il a été scellé par une marque (estampille électronique) sur le poste du votant[2] avant chiffrement sous la clef de l'urne. Cette estampille garantit l'authenticité (habilitation) et l'intégrité (inaltérabilité) du bulletin.

2 Le verrouillage a lieu entre le remplissage et la confirmation. Voir critère (3-conformité). La confirmation a lieu sur la version verrouillée; la syntaxe transmise à l'affichage n'est pas identique à celle pour le remplissage (bien qu'homologique). De plus, l'affichage peut être effectué par une voie distincte.

Cette estampille a été construite avec une étape d'anonymisation empêchant qu'elle soit reliée à un votant spécifique reconnaissable, tout en garantissant être représentante authentique d'un certain votant individuel[3].

↑critères

Pour répondre au critère (8) - prouvabilité :

Chaque opération est journalisée, chaque information et chaque étape sont signées par l'entité opérante, chaque acte important donne lieu à l'émission d'un récépissé pour son bénéficiaire (p.ex. l'habilitation se fait après signature électronique de la carte de vote, le dépôt du bulletin est quittancé).

La présence de deux autorités (et du poste du votant comme troisième partie prenante), l'anonymisation et l'intraçabilité, ainsi que le partitionnement strict des informations (p.ex. flux disjoints entre transactions nominalement identifiées et transactions anonymement authentifiées) permet la preuve de bonne fin -dépôt du bulletin intact- sans révélation du secret du vote.

↑critères

Pour répondre au critère (9) - transparence :

Le critère de transparence fait partie de l'usage établi du vote démocratique (la nécessaire scrutation), mais est aussi une conséquence implicite des deux critères précédents : 7-recomptabilité et 8-prouvabilité.

La transparence statique passe par la publication complète (documentation et texte source électronique), elle est nécessaire[4] pour sa critique et donc sa confiance, mais elle n'est pas suffisante, car le code exécuté peut ne pas être celui étudié.

La transparence dynamique nécessite un second groupe de serveurs participant au protocole de vote, et opérant pour le compte de la commission électorale (scrutation par le contrôle politique).

De surcroit, pour permettre une surveillance distribuée et diffuse dans la population, le poste* du citoyen votant doit être un noeud de passage obligé des transactions du protocole opérant avec l'administration et le contrôle politique.

(*) le logiciel s'exécutant sur le poste du citoyen est sous son contrôle, c'est le seul

3 L'estampille est à la fois la signature numérique du bulletin originel par une clef asymétrique anonyme validée, et la partie publique de cette clef complétée par sa validation (anonymisée) la rendant authentique.

4 Pour être étudié avec efficience, le logiciel doit mettre en oeuvre le plus systématiquement possible des normes usuelles, des algorithmes décrits dans la littérature courante, et se baser sur des bibliothèques standards. Il devrait être aussi fortement calqué sur les principes centraux et les pratiques usuelles du vote, ayant émergé par la nécessité de l'histoire. L'écriture du programme source doit suivre les règles stylistiques et de modularisation (procédurisation contractuelle, encapsulation, types abstraits, ...). Ces modalités permettent alors une compréhension aisée, car pouvant être macroscopique et tirer parti de savoirs antérieurs.

endroit où le public peut être certain que l'exécutable est identique au source étudié - en l'ayant compilé et chargé personnellement.

↑critères

Pour répondre au critère (10) - sécurité :

Ce critère de sécurité[5] explicite une conséquence découlant des trois premiers critères.

Le critère (1-universalité) -vu comme droit d'expression- implique indirectement et partiellement la disponibilité du moyen de vote et son bon fonctionnement; donc la protection contre le sabotage et contre les attaques en déni de service.

Les critères (2-secret) et (3-conformité) impliquent la protection contre des attaques de tiers (piratage) visant à perturber le scrutin, respectivement par prise de connaissance du choix vote, ou par falsification de ce choix.

Au delà, la seule potentialité d'un piratage indétecté, par pré-connaissance[6] ou par falsification, est une attaque virtuelle effective, car elle induit la perte de confiance dans le résultat qui pourrait avoir été manipulé et donc décrébilise le scrutin.

La sécurité contre une attaque dans le protocole est atteinte, d'une part par l'utilisation de normes efficientes et ayant été bien scrutées publiquement, d'autre part par la fondation de l'authentification et de la confidentialité de chaque transactions et de tous les objets importants sur une hiérarchie rigide des clefs cryptographiques.

La sécurité contre le piratage purement technologique se fait tant par la résistance des serveurs eux-mêmes (qualité d'écriture et des outils du logiciels d'application et durcissement des systèmes hôtes), que par leur protection physique et logique, mais aussi par l'isolation de l'ensemble du processus de vote sur le poste du votant (protection contre les maliciels, étanchéité aux traces).

La mitigation d'une attaque sur l'existence du transport (liaison réseau) se fait par le bon usage des protocoles de connection, les possibilitiés de reprises différées et la multiplicité des liaisons possibles.

↑critères

Notes des références légales :

CF34al2 : La Constitution fédérale (art. 34, al. 2) et la jurisprudence constante du Tribunal fédéral (cf. par exemple ATF 121 I 187) protègent la libre formation de l'opinion des citoyens et l'expression fidèle et sûre de leur volonté. Il découle de cette garantie constitutionnelle que les citoyens sont en droit d'exiger que le résultat d'une votation ou d'une élection ne soit pas reconnu s'il n'est pas l'expression fidèle et sûre de la libre volonté des citoyens.
Circulaire du CF 20/09/2002

5 La mitigation du risque se fait soit en diminuant la probabilité d'occurrence du danger, soit en limitant l'étendue du dégât conséquent du danger (pour le rétablir, ou au moins le circonscrire). Ici, cette mitigation se fait soit en empêchant l'attaque, soit en la décelant au plus tôt avant qu'elle n'opère des dégâts, ou de manière à annuler à temps ces dégâts.

6 La pré-connaissance (enfreignant la temporalité-5) permettrait de mobiliser conditionnellement les électeurs opposés aux résultats intermédiaires d'un scrutin. Cette attaque n'est effective que si la durée d'une session est longue (ce qui est d'ailleurs le cas dans le droit actuel -3 semaines).

Visibilité (1) : Le vote traditionnel – y compris le vote par bulletin manuscrit et les fiches de saisie permettant le comptage électronique des voix – repose sur l'existence bien réelle d'un registre électoral, de certificats de capacité civique, de bulletins, de fiches de saisie, d'une urne, de signatures manuscrites, etc. Les endroits où peuvent s'opérer des manipulations sont donc visibles au sens propre, ce qui permet – en cas de panne ou d'abus – d'opérer des contrôles ou des recomptages au vu et au su de chacun.
Rapport du Conseil Fédéral 02.009 sur le vote électronique, chances, risques et faisabilité (p. 16)

Visibilité (2) : "Le vote doit répondre aux principes suivants: suffrage universel, périodicité, égalité, secret, liberté, sécurité et transparence du processus."
"Autre principe à considérer dans la mise en place d'un cadre juridique permettant le vote par internet à distance: la transparence. [...] Cela est d'autant plus important que la dématérialisation accrue du vote pourrait donner une impression d'opacité du processus aux électeurs, ce qui n'est pas compatible avec l'esprit d'une démocratie."
Pour atteindre l'équivalence fonctionnelle de transparence, l'auteur propose trois moyens : "Mise en place d'une chaîne de contrôles", "L'accès au code source du logiciel de vote", "L'audit du processus"
Philippe Mercorio, Faculté de droit - faculté des études supérieures, Université de Montréal

ATF114Ia47 : Les électeurs ont, selon les circonstances, même droit à un recomptage des suffrages qui ont été comptés de manière traditionnelle (ATF 114 Ia 47).
Ibid

↑critères