Le 10 avril 2015

Contre le « vote électronique »
Pour la « consultation électronique »

Temps-réels, section numérique du PS
www.temps-reels.net

Le « vote électronique » présente en l'état des connaissances des risques inacceptables pour la démocratie[1] :

- impossibilité d'éviter les intrusions techniques de tiers malveillants ;
- impossibilité d'assurer l'impartialité de l'autorité organisatrice.

Ceci interdit le « vote électronique » pour les élections politiques : municipales, présidentielles, législatives, européennes. Et pour toute élection jugée « sensible ».

Mais, développer la participation des citoyens aux décisions publiques est un des moyens de lutter contre la crise de légitimité et d'efficacité des représentants dont l'abstentionnisme galopant est l'illustration[2]. La structuration de l'espace du débat et la perspective de devoir prendre position sur une décision prochaine sont alors essentiels à l'implication des citoyens.

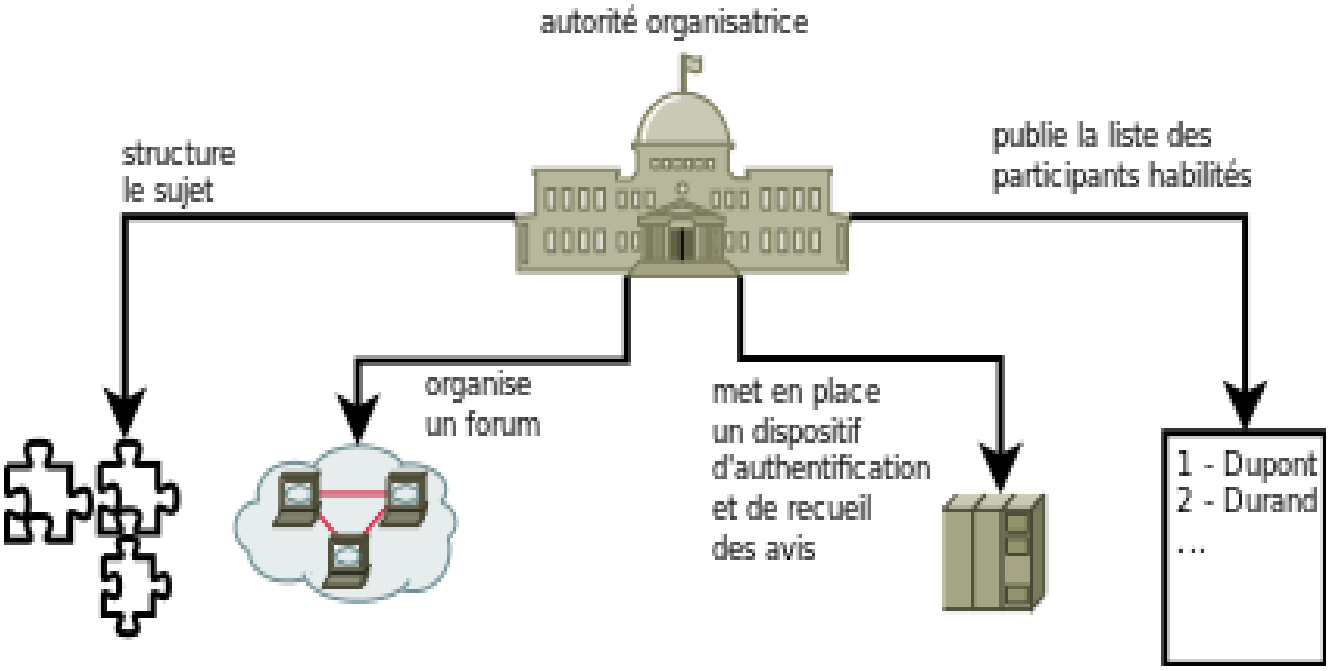
Il convient naturellement d'éviter dans cette démarche les dérives populistes d'un « référendum permanent » qui ne permet pas le recul nécessaire aux décisions et peut ouvrir la voie au mandat impératif[3].

Le numérique permet de multiplier les occasions de participation[4].

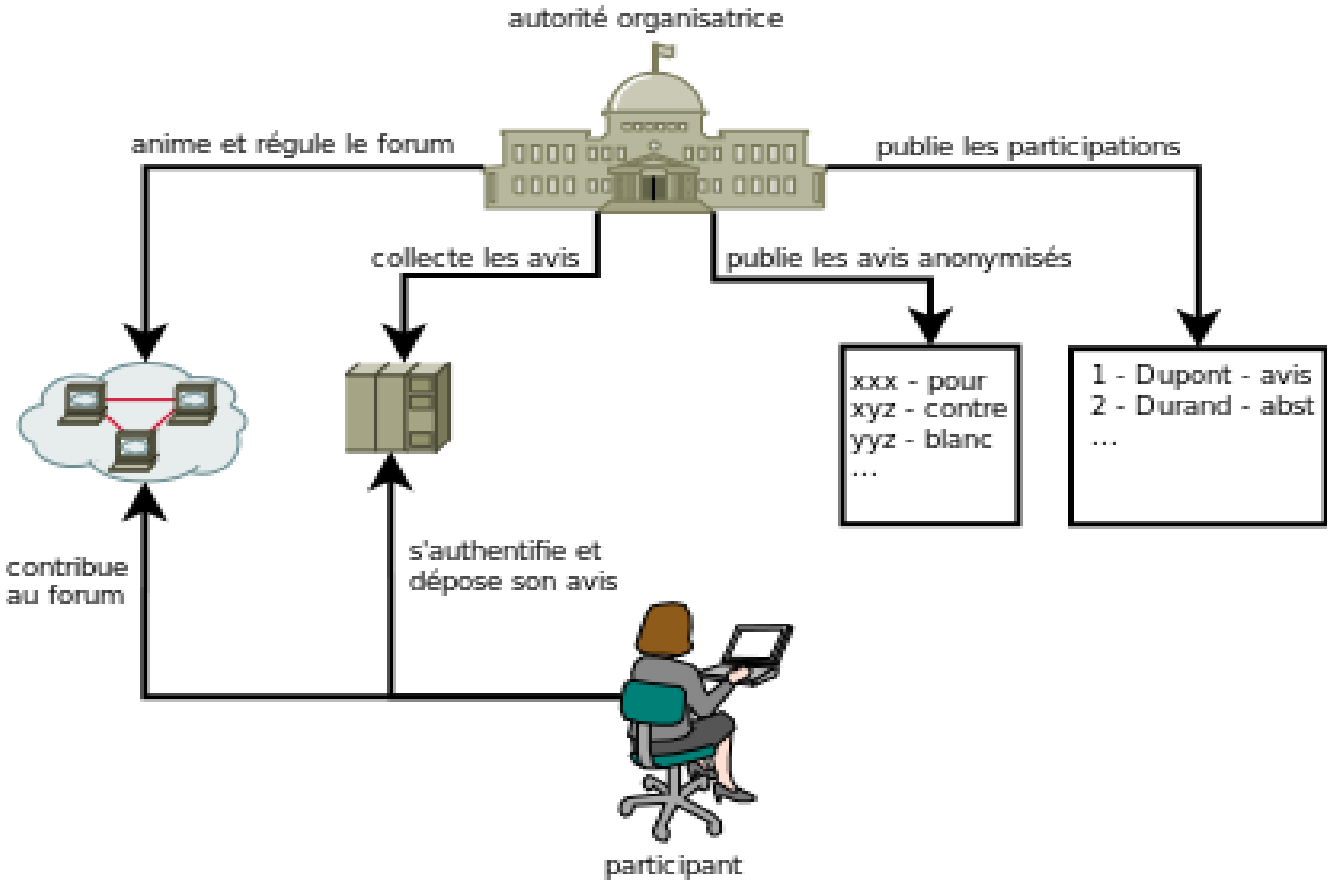
Ce document décrit un dispositif possible de participation aux décisions publiques, limitant les risques liés au numérique.

1 http://hal.inria.fr/docs/01/01/61/44/PDF/RR-8553.pdf
2 www.tnova.fr/essai/d-mocratie-et-soci-t-civile. « Modernisation et ouverture de la pratique démocratique » dans le programme numérique dans le projet socialiste de juin 2011.
3 inconstitutionnel selon l'article 27 de la constitution
4 En particulier, loi organique n° 2013-1114 du 6 décembre 2013 portant application de l'article 11 de la Constitution.

1/ Opérations préalables à la consultation

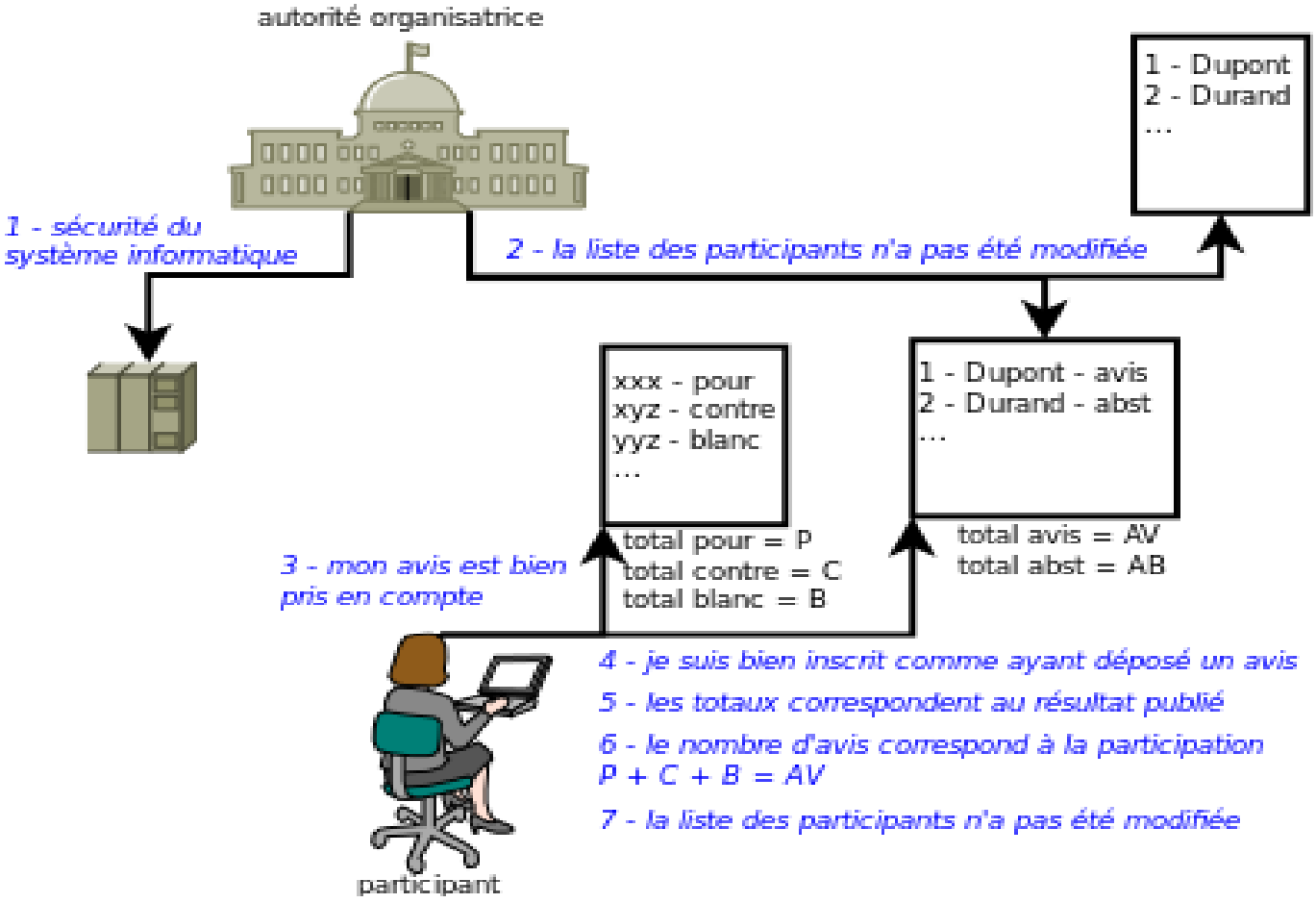


2/ La consultation



La publication des avis et des participations est indispensable au contrôle du dispositif, cf ci-après. Les avis sont anonymisés par un code (xyz ...) choisi par le participant ou délivré par l'autorité, pour ne pas permettre à tout un chacun de constituer des fichiers d'opinions. Ceci ne protège toutefois pas contre la constitution de tels fichiers par l'autorité organisatrice ou un tiers s'introduisant techniquement.

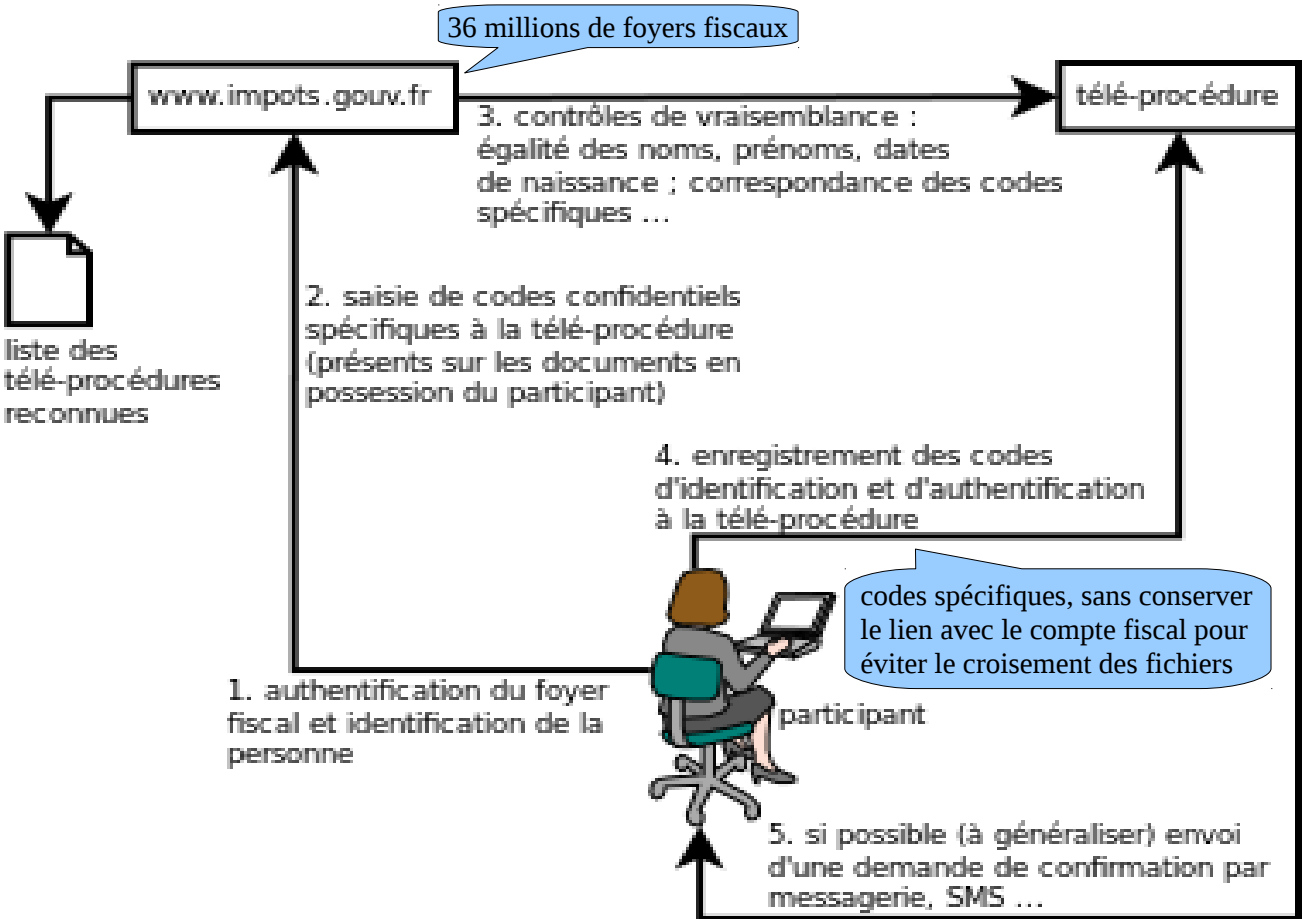
3/ Contrôles



Risque (venant d'une intrusion technique ou d'une manipulation par l'autorité organisatrice)	Réponse (soulignée si insatisfaisante)
Modification de l'avis d'un participant.	Révélé par la vérification de son avis par chaque participant (ctrl 3).
Faire voter un abstentionniste.	Révélé par la vérification de la liste des participants (ctrl 4) par l'abstentionniste.
Publication d'un résultat faux.	Révélé par la vérification du total des avis (ctrl 5).
Ajout d'un avis fictif.	Révélé par la vérification de la correspondance entre le total des avis et le total des participations (ctrl 6).
Ajout d'un avis fictif et d'un participant fictif.	Révélé par la vérification de la liste initiale des participants (ctrl 2 et ctrl 7).
Ajout par l'autorité dès l'origine de personnes fictives dans la liste des participants habilités, puis d'avis fictifs.	Difficile à détecter. Suppose la vérification de la régularité de la liste initiale par des tiers : partis politiques, Conseil constitutionnel ... (par comparaison avec les listes électorales ?).
Constitution de fichiers d'opinions par l'autorité ou par une intrusion technique.	Impossible à détecter. Sauf pour certains cas d'intrusion (ctrl 1). Justifie d'écarter les sujets sensibles.
Intrusion technique visant à discréditer l'autorité en révélant l'avis des participants.	Pas de réponse. Justifie d'écarter les sujets sensibles. Ce risque n'empêche pas la dématérialisation des activités financières, il peut donc être considéré comme limité.

Les mesures d'audit du dispositif, par une autorité obligatoirement indépendante de celle qui l'organise (Conseil constitutionnel, CNIL, citoyens ...), restent à préciser.

4/ Enregistrement d'une authentification



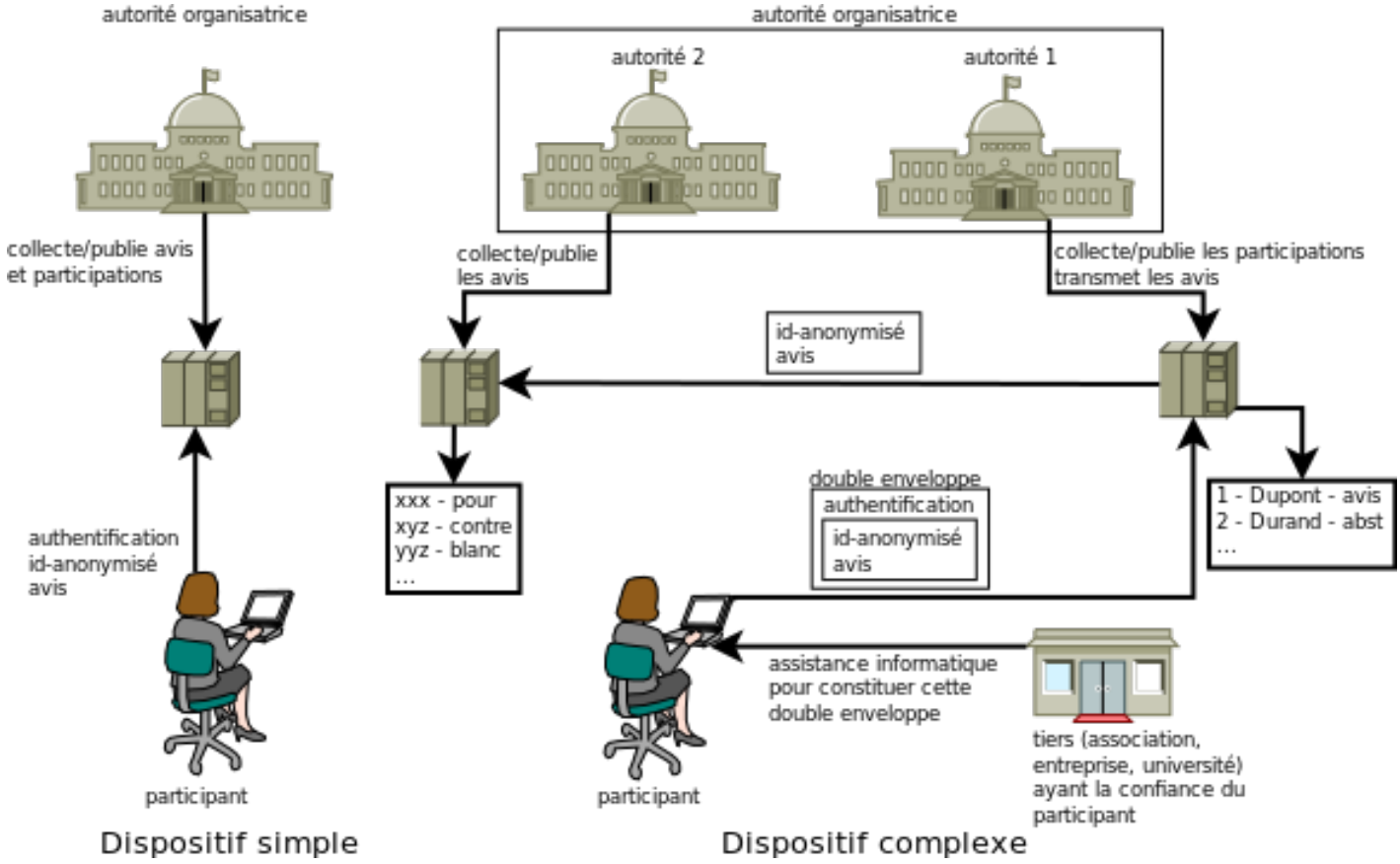
Mécanisme générique pouvant être utilisé pour différentes télé-procédures[5].

Risque	Réponse[6] (soulignée si insatisfaisante)
Usurpation d'identité par un tiers.	Impossible si il n'obtient pas auprès du participant par un moyen détourné (phishing ...) ses codes d'accès à impots.gouv.fr et spécifiques à la télé-procédure.
Usurpation d'identité par un tiers ayant accès aux codes spécifiques à la télé-procédure (garagiste à partir du certificat d'immatriculation du véhicule ...).	Impossible car il ne dispose pas du code d'accès du participant à impots.gouv.fr.
Usurpation d'identité par un tiers ayant accès aux codes spécifiques à la télé-procédure, en utilisant un autre code d'accès à impots.gouv.fr (le sien par exemple).	Impossible car ses nom/prénom/date-de-naissance ne correspondent pas à ceux du participant.
Usurpation d'identité par un tiers ayant connaissance du code d'accès à impots.gouv.fr du participant (agents du fisc, vol de courrier postal).	Impossible car il ne dispose pas des codes spécifiques à la télé-procédure de la personne concernée.
Usurpation d'identité par un autre membre du foyer fiscal.	Possible, en accédant aux documents contenant les codes spécifiques à la télé-procédure. Il court le risque d'être démasqué par l'enregistrement de la date et heure de l'opération.
Usurpation d'identité par l'autorité gérant la télé-procédure.	Possible avec ce type de technique.

5 Début 2014 le rapport Marc ROBERT sur la cybercriminalité fait état de 300.000 usurpations d'identité chaque année, le plus souvent commises en ligne.

6 Le cas d'entités, généralement étatiques, capables d'intrusion massive dans les systèmes informatiques n'est pas traité. Les mécanismes décrit ici ne peuvent pas s'opposer à la possibilité d' usurper les identités que ce moyen leur donne.

5/ Précisions sur le dépôt des avis



Le dispositif simple convient généralement, l'interdiction qui doit être faite à l'autorité de constituer des fichiers d'opinion étant suffisante.

Le dispositif complexe vise, en utilisant une double enveloppe, à préserver le secret des avis de la curiosité de l'autorité. La première est ouverte par l'autorité chargée de collecter et de publier les participations (autorité 1). La seconde contenant l'avis anonymisé est transmise à l'autorité chargée de collecter et de publier les avis (autorité 2). Elle ne peut être ouverte que par cette seconde autorité grâce à un moyen technique[7]. Ainsi, la constitution par l'autorité organisatrice de fichiers d'opinions est rendu plus difficile car elle suppose la complicité de ses deux autorités de mise en oeuvre. Elles doivent être pour cela réellement indépendantes, par exemple en appartenant au Judiciaire pour la collecte des participations et à l'Exécutif pour la collecte des avis. Afin de ne pas dévoiler les avis à la source, l'outil permettant de constituer cette double enveloppe doit être suffisamment simple pour pouvoir être réalisé par un participant averti. Les participants peuvent aussi faire appel à l'assistance informatique de tiers ayant leur confiance, qui leur fourniront souvent une interface en ligne pour déposer leur avis. Seule la multiplicité de ces tiers peut assurer qu'ils ne sont pas subordonnés à l'autorité organisatrice ou à d'autres intérêts. Les mesures visant à limiter leur nombre - par des barrières de certification, de complexité technique artificielle ou de coût d'entrée - doivent donc être évitées. Ce dispositif peut permettre d'engager une protection des données personnelles en consacrant le recours à de multiples tiers indépendants ayant la confiance des internautes et spécialisés dans cette tâche[8]. Compte tenu de la lourdeur de ce dispositif, son intérêt dans le périmètre de ce sujet particulier reste limité.

7 chiffrement par la clé publique de la seconde autorité à priori.

8 ce qui s'inscrirait dans ce que préconise la FING : investir dans les métiers émergents de la confiance : tiers de confiance, agrégateurs et places de marché , "majordomes" numériques, tiers de tiers de confiance, tiers d'évaluation ... http://doc.openfing.org/CONFIANCE/ConfianceNumerique_SyntheseFinale_Fevrier2011.pdf