Fiche reflexe RGPD

« Vote électronique – Vision droit des technologies »

Eric Barbry
Associé
ebarbry@racine.eu

DROIT DE L'IT
DROIT DE L'IP
DONNEES PERSONNELLES

Tel 06 13 28 91 28
Cab 01 44 82 43 00
Mel *ebarbry@racine.eu*
Web www.racine.eu

Eric Barbry
Racine Avocat

ebarbry

Lex numerica

Eric Barbry
Racine Avocat

1. OBJECTIFS

L'article L2122-10-7 du Code du travail prévoit que :

> *« Le scrutin a lieu par voie électronique et par correspondance. Lorsqu'il n'en dispose pas, l'employeur n'a pas l'obligation de mettre à la disposition des salariés le matériel informatique permettant le vote par voie électronique. (…) »*

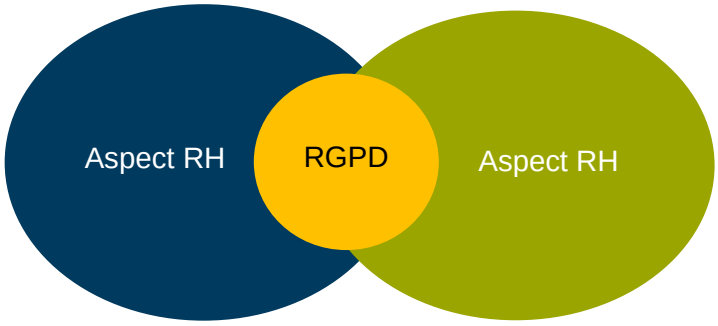
L'article R. 2314-5 du Code du travail précise que :

> *« L'élection des membres de la délégation du personnel du comité social et économique peut être réalisée par vote électronique sur le lieu de travail ou à distance. »*

Au plan juridique il faut décomposer le vote électronique en deux lots :

- le lot purement « RH » qui fixe d'une part le cadre des élections en entreprise et du choix du recours au vote électronique, d'autre part ;
- le lot relatif à ce qu'il est convenu d'appeler le « droit des technologies », à savoir les règles et obligations relatives à l'usage de technologies (solutions de vote) ou aux données traitées (données personnelles notamment).

Nous excluons donc de cette fiche les aspects relatifs à l'organisation des élections elles-mêmes (information obligatoire, protocole préélectoral, établissement des candidats, liste électorale,…).



2. DOCUMENT FONDATEUR

Référentiel - L'article R. 2314-5 du Code du travail précise que :

> *« Sans préjudice des dispositions relatives au protocole d'accord préélectoral prévues aux articles L. 2314-5 et suivants, la possibilité de recourir à un vote électronique est ouverte par un* ***accord d'entreprise ou par un accord de groupe****. A défaut d'accord, l'employeur peut décider de ce recours qui vaut aussi, le cas échéant, pour les élections partielles se déroulant en cours de mandat. »*

Impact – Il ne s'agit pas ici du protocole pré-électoral mais bien d'un document ad hoc sur le seul recours au vote électronique.

Mise en œuvre

- A1 - Proposition d'accord d'entreprise ou accord de Groupe + rédaction dudit accord
- A1bis – A défaut d'accord information du personnel par l'employeur

3. LE CAHIER DES CHARGES

Référentiel - L'article R. 2314-5 du Code du travail précise que :

> *« Un cahier des charges respectant les dispositions des articles R. 2314-6 et suivants est établi dans le cadre de l'accord mentionné au deuxième alinéa ou, à défaut, par l'employeur.*
>
> *Le cahier des charges est tenu à la disposition des salariés sur le lieu de travail. Il est mis sur l'intranet de l'entreprise lorsqu'il en existe un. »*

Impact – Il s'agit ici de rédiger un cahier des charges, c'est-à-dire un document technique qui définisse ce que l'entreprise attend comme « solution » de vote électronique.

Il s'agit d'un cahier des charges « contraint » au sens où ce cahier des charges doit nécessairement respecter les dispositions de l'article R. 2314-6 qui précise que :

> *« Le système retenu* ***assure la confidentialité des données transmises,*** *notamment de celles des fichiers constitués pour établir les listes électorales des collèges électoraux, ainsi que la* ***sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.*** *»*

Un cahier des charges doit nécessairement être rédigé « par l'employeur ».

Il n'est donc pas possible que ce cahier des charges soit rédigé par le prestataire qui fournit la solution de vote électronique lui-même.

A priori ce cahier des charges doit donc être rédigé par la DSI de l'entreprise.

Mais l'employeur (entreprise) ne dispose pas toujours des compétences en interne pour ce faire. Rien ne lui interdit de faire appel à un prestataire extérieur (consultant).

A priori le cahier des charges ne fait pas l'objet d'une démarche particulière après des instances représentatives du personnel. Mais ce même cahier des charges doit être tenu à la disposition des salariés, le texte prévoyant qu'il soit mis sur l'intranet s'il en existe un.

S'il existe un intranet ou un autre espace d'échange numérique avec les salariés, cet espace doit être utilisé mais dans tous les cas une information doit être adressée aux salariés pour les informer que ce cahier des charges existe et peut être consulté.

Mise en œuvre

- A2 : Rédaction du cahier des charges
- A3 – Communication du cahier des charges aux salariés

4. LE CHOIX DU PRESTATAIRE

Référentiel - L'article R. 2314-6 du code du travail précise que :

> *« La conception et la mise en place du système de vote électronique peuvent être confiées à un prestataire choisi par l'employeur sur la base d'un cahier des charges respectant les dispositions du présent paragraphe. »*

Impact – L'employeur peut concevoir et mettre en œuvre sa propre solution de vote. Mais dans la plupart des cas sinon dans la totalité des cas l'entreprise fait appel à un prestataire extérieur.

Ce prestataire pourra soit concevoir et mettre en place, soit simplement mettre en place une solution existante. Dans la plupart des cas les entreprises font appel à un prestataire qui dispose d'une solution de vote électronique qui sera paramétrée aux besoins et contexte du client.

Seule contrainte pour les acteurs privés : le prestataire doit être sélectionné « sur la base du cahier des charges ». Un prestataire qui ne répondrait pas à ce cahier des charges ne pourra donc pas être retenu.

Pour les acteurs publics la contrainte est double : le respect du cahier des charges et les autres critères issus du Règlement de consultation.

Le recours à un prestataire implique deux choses pour l'entreprise :

1. Le choix du prestataire – pour les acteurs privés il s'agit d'un accord de gré à gré cependant le prestataire doit être sélectionné au regard de deux critères précis :

    * Critère 1 – La réponse au Cahier des charges :

* Critère 2 - La conformité au RGPD. Il faut en effet rappeler qu'un prestataire qui traite des données (qualifié de sous-traitant) au sens du RGPD ne peut être retenu que s'il assure au responsable de traitement une conformité au RGPD.

Il est donc nécessaire de prévoir une procédure de sélection et dans tous les cas de communiquer au prestataire un questionnaire de conformité RGPD et une annexe contractuelle RGPD.

2. Le contrat avec le prestataire. C'est sans doute l'élément le plus important de l'opération. Or souvent les contrats sont des contrats « standards » proposés par les éditeurs de solution de vote électronique et qui sont donc plus protecteurs des intérêts de l'éditeur que ceux de l'entreprise cliente.

Il importe donc, dès la phase amont de sélection, de préciser que le contrat utilisé sera celui du client soit que le contrat de l'éditeur de la solution fera nécessairement l'objet d'une négociation et doit être communiqué au client en même temps que la réponse au cahier des charges.

En termes de localisation de la solution, la Cnil préconise dans sa délibération du 21 octobre 2010 que *« les serveurs et les autres moyens informatiques centraux du système de vote électronique soient localisés sur le territoire national afin de permettre un contrôle effectif de ces opérations par les membres du bureau de vote et les délégués ainsi que l'intervention, le cas échéant, des autorités nationales compétentes ».*

Mise en œuvre

- A4 – RFI (request for interest) + pré-requis juridique pour sélection du candidat + pré-requis RGPD en sa qualité de sous-traitant
- A5 – Rédaction (négociation) du contrat avec le prestataire

5. EXPERTISE INDEPENDANTE

Référentiel – L'article R. 2314-9 précise que :

« Préalablement à sa mise en place ou à toute modification substantielle de sa conception, le système de vote électronique est soumis à une expertise indépendante destinée à vérifier le respect des articles R. 2314-5 à R. 2314-8. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Les prescriptions de ces mêmes articles s'imposent également aux personnes chargées de la gestion et de la maintenance du système informatique. »

Impact – Cet article n'est pas clair dans sa formulation. La question souvent posée est de savoir si l'expertise indépendante doit être réalisée à l'initiative de l'entreprise ou si elle peut être communiquée à ses clients par le prestataire de vote électronique lui-même.

La formule « préalablement à sa mise en place » laisse penser que c'est bien à l'employeur de faire réaliser une expertise indépendante sur la solution retenue.

La délibération de la Cnil n°2010-371 du 21 octobre 2010 milite également en ce sens en imposant un spectre large à cette expertise indépendante :

« L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc,.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc). »

Concernant l'indépendance, la Cnil précise qu'en dehors de la compétence technique (sécurité notamment), l'expert ne doit pas avoir « d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d'utiliser cette solution ».

Sur l'étendue de l'expertise il faut être très attentif car le texte précise bien que l'expertise doit porter sur le respect des articles R. 2314-5 à R. 2314-8. Or si certains articles sont purement techniques (R. 2314-8 et partiellement R. 2314-7 et R. 3214-6), les autres articles sont liés à l'organisation du vote lui-même : accord ou non, cahier des charges, sélection du candidat,…

Paradoxalement, l'expertise doit aussi porter sur le respect des dispositions de l'arrêté du 25 avril 2007.

De fait cet audit ne peut pas uniquement porter sur la partie technique et fonctionnelle de la solution mais repose sur un spectre beaucoup plus large dont une bonne partie est juridique.

Ce spectre large de l'audit témoigne une fois encore qu'une expertise indépendante communiquée par l'éditeur de la solution ne parait pas répondre aux exigences du code.

Mise en œuvre

- A7 – Choix de l'expert indépendant et contractualisation
- A8 – Rédaction d'un accord de méthode entre le client et le prestataire pour définir les conditions d'intervention de l'expert indépendant
- A9 – Réalisation et restitution de l'audit
- A10 – Mis en œuvre s'il y a lieu des préconisations de l'auditeur pouvant aller jusqu'à la résolution du contrat. Ce point est important car il doit nécessairement figurer dans le contrat qui lie l'entreprise à son prestataire (clause résolutoire en cas de rapport aboutissant à la non-conformité de la solution)

6. ANNEXE AU PROTOCOLE PREELECTORAL

Référentiel – L'article R. 2314-14 dispose que :

« Le protocole d'accord préélectoral mentionne la conclusion de l'accord d'entreprise ou de l'accord de groupe autorisant le recours au vote électronique et, s'il est déjà arrêté, le nom du prestataire choisi pour le mettre en place.

Il comporte en annexe la description détaillée du fonctionnement du système retenu et du déroulement des opérations électorales. »

Impact – Là encore il s'agit d'assurer la plus grande transparence sur les aspects techniques, fonctionnels et organisationnels du vote. Le texte impose donc que figure en annexe un document ad hoc détaillé.

Cette annexe peut être communiquée par le prestataire lui-même mais dans un tel cas elle devra être contextualisée au regard de la procédure mise en œuvre dans l'entreprise.

Mise en œuvre

- A11 – Rédaction de l'annexe

7. CELLULE D'ASSISTANCE TECHNIQUE

Référentiel - L'article R. 2314-10 dispose que :

> *« L'employeur met en place une cellule d'assistance technique chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique, comprenant, le cas échéant, les représentants du prestataire. »*

Impact – Pour assurer le bon déroulé du vote l'employeur doit mettre en place une cellule d'assistance technique comprenant des membres du personnel de l'entreprise, et si un prestataire a été choisi, des représentants de ce prestataire.

La mission de la cellule d'assistance technique est cruciale. Il est prévu notamment à l'article R. 2314-15 qu'elle doit procéder à un certain nombre d'opérations :

> *« En présence des représentants des listes de candidats, la cellule d'assistance technique :*
>
> *1° Procède, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifie que l'urne électronique est vide, scellée et chiffrée par des clés délivrées à cet effet ;*
>
> *2° Procède, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement à l'issue duquel le système est scellé ;*
>
> *3° Contrôle, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système. »*

Mise en œuvre

- A12 – Désignation des membres de la cellule d'assistance technique
- A13 – Méthodologie « Cellule d'assistance technique » qui définit les rôles et missions de la Commission et les limites de son intervention
- A14 – Formation des membres de la Cellule d'assistance technique

8. INFORMATION ET FORMATION

Référentiel – L'article R. 2314-12 dispose que :

« Chaque salarié dispose d'une notice d'information détaillée sur le déroulement des opérations électorales.

Les membres de la délégation du personnel et les membres du bureau de vote bénéficient d'une formation sur le système de vote électronique retenu. »

Impact – Il s'agit là d'assurer la plus grande transparence à l'égard des salariés et de permettre à leurs représentants ou aux personnes en charge du scrutin (membre du bureau de vote) de disposer de la formation nécessaire pour maîtriser le vote d'une part et répondre le cas échéant aux questions des salariés.

Mise en œuvre

- A15 – Rédaction de la notice d'information détaillée
- A16 – Envoi aux salariés de la note d'information
- A17 – Formation des membres de la délégation du personnel et des membres du bureau de vote

9. RESPECT DU DROIT DES DONNEES A CARACTERE PERSONNEL

Référentiel – Dans sa rédaction actuelle, l'article R. 2314-11 rappelle que :

« L'employeur informe les organisations syndicales de salariés représentatives dans l'entreprise ou dans le ou les établissements concernés, de l'accomplissement des formalités déclaratives préalables auprès de la Commission nationale de l'informatique et des libertés. »

Par ailleurs, il faut rappeler que l'article R. 2314-9 impose que le rapport d'expertise indépendante soit *« tenu à la disposition de la Commission nationale de l'informatique et des libertés ».*

Il faut rappeler que l'article 4 du décret 25 avril 2007 fixe les catégories de données pouvant être collectées et que l'article 5 fixe la liste des destinataires ou catégories de destinataires.

Impact – Depuis l'adoption du RGPD il n'y a plus de démarche préalable auprès de la Cnil (hors cas particuliers comme les analyses d'impact ou certains traitements visés dans la loi) mais l'ensemble des autres obligations doivent être respectées.

Mise en œuvre – Sans entrer dans le détail, l'entreprise qui met en œuvre une procédure de vote électronique devra assurer :

- A18 – Saisine du DPO s'il en existe un
- A19 – Ajout au registre des traitements s'il y a lieu
- A20 – Information des personnels soit dans le cadre de sa politique de données salariés, soit dans un document spécifique ;

- A21 – Gestion du prestataire : sélection / contrat adapté / démarches de fin de contrat
- A22 – Impératif de sécurité partagé avec le prestataire
- A23 – Mise en œuvre d'une démarche « privacy by design »
- A24 – Gestion de l'exercice des droits par les personnes concernées
- A25 – Gestion des flux transfrontières s'il y a lieu

10. TRACABILITE

Référentiel – L'article R. 2314-7 précise que :

> *« Lors de l'élection par vote électronique, les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne sont uniquement accessibles aux personnes chargées de la gestion et de la maintenance du système. »*

L'article R. 2314-16 impose une autre obligation qui dispose que « la liste d'émargement n'est accessible qu'aux membres du bureau de vote et à des fins de contrôle de déroulement du scrutin ».

Impact – Il s'agit là d'assurer que seules les personnes en charge de la gestion et de la maintenance du système auront accès à des éléments critiques.

Mise en œuvre

- A26 – Dresser la liste des « personnes en charge de la gestion et de la maintenance du système » qui doit être une liste fermée ;
- A27 – Définir les droits d'accès (politique d'habilitation) et les conditions de traçabilité (politique de traçabilité) de ces personnes ;
- A28 – Si ces personnes sont des salariés d'un sous-traitant (ce qui est généralement le cas), il importe en application de l'article 28 du RGPD qu'ils soient tenus à un engagement de confidentialité renforcé (ce point doit être prévu dans l'annexe RGPD).

11. DEMARCHE D'AUDIT

Référentiel – L'article 3 de l'arrêté du 25 avril 2007 précise que :

> *« Toutes les mesures sont prises pour leur (représentant de l'entreprise mettant en place le vote) permettre de vérifier l'effectivité des dispositifs de sécurité prévus ».*

Par ailleurs, le RGPD impose au responsable de traitement de définir et le cas échéant de mettre en œuvre les mesures d'audit appropriées (y compris par inspection).

Impact – Le process de vote électronique se doit d'être auditable sur deux plans : l'audit du process par les personnes, internes à l'entreprise en charge du vote ; l'audit du prestataire externe en charge du vote. Rappelons que le RGPD envisage différentes formes d'audit dont des audits dit « d'inspection ».

Mise en œuvre

- A29 – Dans le cadre de l'accord d'entreprise ou de l'annexe au protocole pré électoral il convient de prévoir la démarche permettant aux personnes en charge de l'élection de procéder à tout contrôle ou toute vérification elles estimeraient nécessaires. Cette procédure doit nécessairement être écrite et documentée.
- A30 – Dans le cadre du contrat qui lie l'entreprise au prestataire il importe de prévoir les conditions d'audit, notamment au regard du respect du RGPD mais plus généralement des engagements contractuels.

Lorsque l'entreprise dispose d'une direction de l'audit ou de la conformité, cette dernière doit être saisie.

12. GESTION DE CRISE

Référentiel – L'article 3 de l'arrêté du 25 avril 2007 précise que :

> *« En cas de dysfonctionnement informatique résultant d'une attaque du système par un tiers, d'une infection virale, d'une défaillance technique ou d'une altération des données, le bureau de vote a compétence, après avis des représentants susmentionnés, pour prendre toute mesure d'information et de sauvegarde et notamment pour décider la suspension des opérations de vote. »*

Le RGPD quant à lui impose en cas de violation de sécurité différentes mesures : mise en œuvre de mesures de réaction, rapport d'incident ou encore notification à la Cnil et au besoin information des personnels.

Rappelons que la Cnil dans sa délibération du 21 octobre 2010 précise que *« tout système de vote électronique doit comporter un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques ».*

Impact – Les dispositions propres au droit du vote électronique tout comme celles relatives au droit des données personnelles (RGPD notamment) imposent de savoir appréhender correctement une violation de sécurité

Mise en œuvre

- A31 – Intégrer la procédure de vote électronique dans le process de cellule de crise de l'entreprise
- A32 – A défaut de cellule de crise organisée, rédaction dans l'annexe au protocole pré-électoral des conditions de réaction en cas d'attaque

13. CONSERVATION ET DESTRUCTION

Référentiel – L'article R. 2314-17 précise que :

« L'employeur ou le prestataire qu'il a retenu conserve sous scellés, jusqu'à l'expiration du délai de recours et, lorsqu'une action contentieuse a été engagée, jusqu'à la décision juridictionnelle devenue définitive, les fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde. La procédure de décompte des votes doit, si nécessaire, pouvoir être exécutée de nouveau.

A l'expiration du délai de recours ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive, l'employeur ou, le cas échéant, le prestataire procède à la destruction des fichiers supports. »

Impact – Cet article impose une double contrainte :

- Une obligation de conservation pendant la durée des voies de recours et en cas de contentieux tout le temps de celui-ci ;
- Une obligation de suppression passé les délais en question.

Mise en œuvre

Sur l'obligation de conservation, il convient de définir les conditions de conservation sur un plan juridique comme sur un plan technique.

- A33 – Au plan technique, rédaction d'une « Politique de conservation »
- A34 – Au plan juridique, rédaction d'une convention de preuve incluse ou annexée dans l'accord d'entreprise s'il en existe un

14. ASSURANCE

Référentiel – Il n'existe pas de référentiel particulier sur le sujet mais la question de l'assurance relative à la mise en œuvre de ce type de process doit être posée au regard de conséquences possibles (financières ou d'image) pour l'entreprise

Impact – Il faut ici raisonner aussi bien au niveau de l'entreprise qui met en œuvre la procédure qu'au niveau de la responsabilité de son prestataire.

Mise en œuvre

- A35 – Contrôle de la police d'assurance de l'entreprise
- A36 – Contrôle des attestations d'assurance du prestataire