RÉVERSIBILITÉ DES DONNÉES ET ARCHIVAGE

Amélie Vernusset

A.D.B.S. | « I2D – Information, données & documents »

2015/3 Volume 52 | pages 17 à 18

ISSN 2428-2111

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-i2d-information-donnees-et-documents-2015-3-page-17.htm

Réversibilité des données et archivage

[conservation] La réversibilité des données des systèmes d'information sécurise la fonction de conservation des documents. La non réversibilité étant un risque, l'article donne des conseils méthodologiques pour s'en prémunir et souligne l'apport des professionnels de la gestion des documents dans la maîtrise de ce risque.

Les entreprises accélèrent la dématérialisation de leurs processus pour s'adapter aux pratiques de leurs clients et partenaires mais aussi pour gagner en efficacité et donc en coût. Cette mutation leur demande d'adapter la gestion de leurs documents. Elles doivent s'assurer de la conservation sécurisée de leurs documents d'activité sur de longues périodes, se comptant parfois en dizaines d'années. Elles font le choix de conserver les documents numériques soit dans des systèmes d'information spécifiques comme les systèmes d'archivage électroniques (SAE) ou les logiciels de gestion électronique de documents (GED), soit dans des systèmes métier comme les systèmes de gestion ou les systèmes de ressources humaines, une combinaison des deux étant possible.

Les entreprises doivent s'assurer du maintien de l'intégrité, de l'authenticité et de la disponibilité des documents numériques dans le temps. Cela implique d'être en mesure de gérer les documents au-delà des évolutions des systèmes d'information. En effet, ceux-ci évoluent régulièrement et peuvent être abandonnés au profit d'autres systèmes pour répondre aux besoins des utilisateurs, aux choix stratégiques et aux contraintes des entreprises[1]. Celles-ci doivent donc être en capacité de migrer leurs documents d'activité d'un système à un autre. Cette « réversibilité » peut se définir comme la capacité à restituer à leur propriétaire les documents conservés ainsi que les données nécessaires pour garantir l'intégrité et l'authenticité des documents de façon sécurisée.

Les risques en cas de non réversibilité d'un système

Si un système est non réversible, une entreprise court le risque de ne pas pouvoir récupérer ses documents et les données qui les accompagnent. Le risque est donc documentaire et la non disposition des documents peut mettre en péril la poursuite de ses activités, lors d'un audit réglementaire ou lors d'un contentieux par exemple. Face à un système non réversible, l'entreprise est face à trois choix :

- maintenir un système inadapté ou obsolète,
- développer des outils rendant la sortie possible avec des pertes partielles,
- accepter de perdre les documents.

Dans le premier cas, l'entreprise devra payer le maintien d'une solution jusqu'à la fin de la période de conservation des documents, ce qui entraînera un coût supplémentaire, difficilement maîtrisable. Dans le deuxième cas, elle devra payer le développement des outils nécessaires et accepter une récupération dégradée ; elle sera donc face à un risque à la fois financier et documentaire. Dans le troisième cas, elle devra assumer un risque documentaire, sans être en mesure de chiffrer l'impact de cette perte.

Face à un problème de réversibilité, il est possible de combiner les solutions palliatives, par exemple en maintenant le système pendant plusieurs années pour minimiser le risque de non disposition des documents ou en développant des outils uniquement pour les documents identifiés comme majeurs. Cependant, ces choix ne peuvent pas être une solution satisfaisante. Pour éviter de se retrouver dans une telle situation, il est indispensable d'anticiper le risque de non réversibilité à chaque phase d'un projet de système d'information.

Maîtriser le risque de non réversibilité

La norme ISO 31000:2009 définit le risque comme « *l'effet de l'incertitude sur les objectifs* » et précise qu'il est « *souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux* ». Pour maîtriser le risque de non réversibilité, il convient donc d'identifier les objectifs, c'est-à-dire les documents et données à récupérer en cas de sortie du système, quelle qu'en soit la raison (événement), et d'identifier les conséquences en cas de non restitution de ceux-ci.

Dans le cadre de la mise en place d'un système d'information gérant des documents d'activité, la première étape consiste donc à définir ce qui sera à récupérer à la sortie du système pour permettre ////

1. Amélie Vernusset. « La réversibilité dans un système d'archivage électronique ». Partie 1 (20 janvier 2015), partie 2 (27 janvier 2015), partie 3 (6 février 2015). Consultable sur le blog « Records management is the new black » https://lotteauxfraises.wordpress.com

//// la disposition des documents dans le temps. L'exploitation des documents d'activité nécessite de conserver la preuve de leur authenticité et de leur intégrité. Il convient donc au minimum de récupérer les documents d'activité, c'est-à-dire les documents eux-mêmes et leurs métadonnées. Il peut également être nécessaire de récupérer les éléments de preuve complétant les documents. Ces éléments peuvent être spécifiques à chaque document ou dossier (certificat de signature électronique, piste d'audit) ou commun (documentation du système, description des jeux de métadonnées, historisation des événements survenus, traces des destructions, etc.) et les liens entre tous les éléments restitués. Le niveau d'exigence dépendra de la nature des documents conservés (copie, original) et de la finalité de la conservation. En effet, des documents conservés à titre de mémoire institutionnelle ne demanderont pas le même niveau d'exigence que des contrats signés électroniquement, par exemple.

S'il convient de prévoir la possibilité de sortir d'un système d'information, il convient également de prendre en compte le besoin de réversibilité lors des évolutions du système. Cela signifie de prendre en compte l'impact de chaque évolution sur la capacité ultérieure à sortir du système. Cela permet de choisir les solutions les plus efficaces et d'écarter les évolutions qui représentent un risque de non réversibilité. Cela peut entraîner des contraintes lors de la mise en œuvre de l'évolution ou un développement supplémentaire afin de garantir la disposition des documents dans le temps au-delà du cycle de vie des systèmes. Par exemple, s'il y a une évolution d'un profil d'archivage utilisé pour l'attribution de métadonnées ou des niveaux de sécurité différents, il sera préférable de choisir de créer un nouveau profil plutôt que de faire évoluer celui existant pour éviter de devoir reprendre l'historique de cette évolution au moment de la sortie du système.

Pour garantir le maintien de l'authenticité et de l'intégrité des documents lors de la sortie d'un système, il conviendra de définir les exigences à respecter[2]. Ici aussi, elles dépendront de la nature des documents et de la finalité de leur conservation et seront souvent corrélées au niveau d'exigences vis-à-vis du système lui-même. La migration sera gérée comme un projet à part entière. L'analyse des besoins et le cahier des charges devront intégrer la problématique de la réversibilité et le plan de migration devra définir au minimum :

- les éléments à récupérer (documents, métadonnées, liens, etc.),
- les modalités de restitution (l'attribution d'identifiant unique au lot de migration, les conditions physiques de sécurité, etc.),
- les modalités de destruction,
- les modalités de transfert dans le nouveau système (reprise de toutes les métadonnées, historisation des événements passés, etc.),
- les modalités de test (afin de vérifier que tout est bien transféré avant destruction, puis détruit).

Le problème de la réversibilité des systèmes est avant tout un problème de sécurité des systèmes d'information et doit donc faire partie des points d'attention des spécialistes de la sécurité. Pourtant, les spécialistes de la gestion des documents sont indispensables pour que le risque documentaire soit pris en compte de façon satisfaisante.

L'apport des professionnels de la gestion des documents

Les professionnels de la gestion des documents peuvent avoir la casquette de documentaliste, archiviste, chef de projet SAE/GED, consultant fonctionnel, records manager. Dans tous les cas, ce seront eux qui pourront accompagner leur entreprise ou administration dans l'étude des besoins, les modalités d'évaluation des solutions, l'évaluation des solutions elles-mêmes, la prise en compte au niveau contractuel de la réversibilité, les choix d'évolution, l'analyse des besoins lors d'une migration, etc.

Leurs compétences et leurs méthodes de travail (référentiel de conservation, cartographie documentaire, audits documentaires, etc.) leur permettent en effet :

- d'identifier les systèmes d'information concernés par les risques de non réversibilité spécifiques aux documents d'activité, que ce soient des systèmes existants et à venir,
- d'analyser les besoins de maintien de l'authenticité et de l'intégrité des documents,
- d'alerter sur les risques de non réversibilité d'un système (en cas d'absence d'identifiant unique, par exemple),
- d'être vigilant sur la capacité réelle d'un système et de demander des tests et éléments de preuve de réversibilité,
- de tenir compte des cycles de vie des documents, souvent plus longs que les cycles de vie des systèmes.

Après cet exposé sur les risques de non réversibilité et la façon de s'en prémunir, on pourrait se demander s'il est réellement possible d'en maîtriser toutes les composantes. Dans ce domaine comme dans les autres, le risque zéro n'existe pas. Pourtant, si l'on intègre cette problématique tout au long d'un projet, nous pouvons minimiser ce risque et faire en sorte que les projets soient menés en intégrant la gestion des documents à long terme, indépendamment des cycles de vie des systèmes d'information. En tant que professionnel de la gestion des documents, nos compétences nous permettent de jouer le rôle de conseiller et de prescripteur pour accompagner les entreprises dans leur gestion des risques, à côté des spécialistes de la sécurité et des juristes. ■

> **Amélie VERNUSSET**
Consultante, GDoc Lasercom
amelie.vernusset@gdoc-lasercom.com
www.linkedin.com/in/avernusset/fr

2. Marie Demoulin, Amélie Vernusset. « La réversibilité des données et l'archivage électronique ou comment éviter la dépendance technologique », *Les Cahiers du Numérique*, 2015, n°2, p.115-148