

# Gare aux archives numériques !

Les echos : 21/04/11 Laurence Neuer

Dans l'entreprise, le tri sélectif, c'est aussi l'affaire des informaticiens. Que faut-il garder parmi les milliards de données stockées sur les serveurs, dans les messageries et les postes informatiques des salariés ? L'enjeu est considérable, à l'heure où la France se met à l'« e-discovery ». Ce terme générique est emprunté à la procédure américaine du même nom. Il vise toutes les situations dans lesquelles l'entreprise se retrouve contrainte de produire des documents électroniques.

Les occasions d'avoir à se justifier ne cessent de se multiplier. Soupçons de falsification, de détournement, d'entente frauduleuse, dénonciations : les enquêtes judiciaires ou administratives sont nombreuses et comportent des risques pour l'entreprise.

« *Le directeur informatique a tendance à tout conserver. Mais l'entreprise doit prendre conscience que l'information peut aussi nuire à ses intérêts. Elle peut resurgir à tout moment et contre son gré* », prévient Catherine Leloup, secrétaire générale de l'Association française de l'audit et du conseil informatiques (Afaï). Dans ces conditions, que jeter, que garder et pendant combien de temps ? L'arbitrage est d'autant plus délicat que de bonnes raisons plaident pour des choix contradictoires : réduire les coûts et désengorger le système, d'un côté ; justifier de ses droits en cas de conflit ou de contrôle, de l'autre.

## 1. Détruire les données non nécessaires

Une entreprise de travaux publics est soupçonnée de corruption. Ses dirigeants reçoivent la visite surprise d'agents de la police judiciaire chargés de l'enquête pénale. S'ensuivent une perquisition et la saisie de supports informatiques dans ses murs. Au détour d'une pièce jointe dans un e-mail, un enquêteur épingle un élément laissant présumer une fraude fiscale. « *Une fois qu'il est rentré dans le système informatique, l'enquêteur peut voir des choses qu'il ne cherchait pas et rien ne lui interdit de les communiquer aux services fiscaux* », indique Isabelle Renard, avocate associée au cabinet Racine. L'entreprise avait sousestimé les effets délétères de sa mémoire numérique face aux pouvoirs d'enquête très étendus des services de police. Il a suffi de quelques clics pour que son réflexe de « conservation » devienne le pire des mouchards. « *La messagerie est un immense piège, note Catherine Leloup. Archiver, c'est aussi détruire.* »

## 2. Attribuer des durées de vie aux documents

Loin de l'image poussiéreuse que le mot suggère, l'« archivage » abrite la mémoire numérique de l'entreprise, indispensable pour justifier de ses droits. Factures, bulletins de paye, documents comptables ou contrats commerciaux, notamment, doivent être conservés plusieurs années.

Cet archivage « légal » ou « à valeur probatoire » permet non seulement de montrer patte blanche en cas de contrôle, mais aussi de se défendre dans une instance. L'entreprise aura par exemple intérêt à conserver les preuves de ses factures et contrats pendant cinq ans, durée de la prescription en la matière. « *D'une manière générale, les entreprises attribuent des durées de conservation globales aux documents en fonction de leur nature* », explique Isabelle Renard. Nombre d'entre elles sont aussi concernées par le droit à l'oubli numérique, qui impose aux responsables des fichiers de détruire les données personnelles qu'ils gèrent au bout d'un certain temps.

## 3. Répartir l'information en catégories

La conservation et le classement de l'information s'inscrivent désormais dans une stratégie dictée par les besoins de l'entreprise. D'abord, il faut se demander pourquoi le document est archivé. Peut-être s'agit-il de répondre à une obligation légale ? A moins que le but ne soit d'immortaliser le processus de production ou de mémoriser les opérations visant à anticiper un risque sur la santé publique. Ensuite, il convient de se demander comment : faut-il archiver ses documents en interne ou les externaliser ? Dans ce dernier cas, le sous-traitant doit être en mesure de garantir l'évolution de son système d'archivage et la restitution des données en fin de contrat. De véritables politiques d'archivage sont mises en place dans les entreprises qui répartissent l'information en catégories :

« légale », « réglementaire », « historique » et « stratégique » - cette dernière abritant tout ce qui n'entre pas dans les autres catégories. Toute la finesse est de définir une politique en amont de façon à pouvoir justifier, lors d'un éventuel contrôle, la destruction des documents. Une telle démarche aurait épargné à Arthur Andersen son inculpation pour entrave à la justice et destruction de preuves dans l'affaire Enron. « *Les données qui ne rentrent dans aucune catégorie, il est fortement recommandé de les détruire* », préconise Isabelle Renard.

#### **à retenir**

- L'archivage doit répondre à trois objectifs : réduction des coûts, obligation légale, conservation des preuves.
- La loi fixe des dates de péremption des données personnelles, sanctions pénales à la clef, et la CNIL veille.
- En justice, la valeur de preuve d'une information numérique est fragile, d'où l'importance de mettre en oeuvre des moyens techniques assurant sa sécurité, son intégrité et sa lisibilité tout au long de son cycle de vie