

Confidentialité *versus* accès

Intervenant

Bruno DANVIN, responsable de la Mission Archivage, Conservation, Traçabilité des Données au sein de GDF SUEZ

Divulgence des données confidentielles

Les documents ou données confidentiels sont à l'image de tous les autres : à de très rares exceptions, il faut pouvoir les lire.

La différence, c'est que ces documents ne doivent circuler qu'entre certaines personnes, des personnes de confiance. Cela suppose que l'on ait au préalable défini précisément ce qu'était le cercle de confiance (une liste de noms ou de fonctions). La divulgation, c'est quand le document sort de ce cercle, que ce soit de manière consciente ou accidentelle.

Il ne faut pas confondre la notion de confidentialité avec d'autres notions.

D'abord la durée de conservation : des documents peuvent être confidentiels pour une durée courte ; avant le lancement public d'un projet innovant, la préparation d'achat ou de vente d'une entreprise, une fusion etc... A l'inverse, des documents doivent être conservés longtemps même s'ils ne sont pas ou plus confidentiels : les données publiques concernant l'activité, les finances d'une organisation.

Une autre confusion est celle qui associe confidentialité et importance, je n'ose ici dire valeur du document. Pour reprendre l'exemple du bilan financier, celui-ci, une fois publié selon les lois du pays, devient à la fois un document public et très important pour celui qui sait l'analyser. Une erreur classique est de considérer que ce que l'on fait est important et donc confidentiel. Les choses sont un peu plus compliquées...

Outre le fait qu'il n'y a pas de lien de causalité entre durée et confidentialité, importance et confidentialité, la valeur confidentielle de tel ou tel document ou donnée évolue également dans le temps. Tel document confidentiel un temps ne l'est plus au bout d'un certain temps ; il peut même arriver, mais c'est plus rare, qu'un document jugé non confidentiel au moment de son élaboration le devienne.

Tout ceci pour dire que, plus que pour tout autre document, les documents confidentiels doivent être gérés soigneusement.

Bien sûr, il y a plusieurs niveaux de confidentialité, le niveau ultime étant le document non répertorié – les notes blanches – mais cela doit rester très exceptionnel.

Considérer la notion de confidentialité en tant que telle, gérer dans le temps la liste de diffusion des documents confidentiels suppose une culture partagée de l'information confidentielle. La prise de conscience du risque engendré par la diffusion d'une information confidentielle suppose aussi que les processus de mise en confidentialité d'un document et de sa gestion soient précisés et diffusés.

Les difficultés ont fortement augmenté avec le numérique. Il ne suffit pas de limiter l'accès à un nombre déterminé de personnes et de protéger cette barrière, il faut aussi empêcher la copie, y compris l'image de l'écran d'ordinateur sur lequel apparaît le document.

Pourtant, dans tous les cas, on en revient à la notion de confiance. Dire, sans même en divulguer le contenu, qu'on est détenteur de documents ou données confidentiels, pour satisfaire son ego, c'est déjà en dire trop.

Pour se garantir de la divulgation des documents confidentiels, il faut donc des personnes dans la confiance, un système de gestion de ces personnes et la possibilité pour un groupe plus restreint, généralement une seule personne désignée, de lever ou non la confidentialité des documents répertoriés.

Open data et protection des données

L'accent que l'on met aujourd'hui sur l'accès public aux données – open data – est, paradoxalement, l'occasion pour les organisations de mieux gérer la protection des données.

Cela pour deux raisons :

- La première, c'est la prise de conscience que nous sommes souvent déjà à livre ouvert vis-à-vis de l'externe. Ne nous y trompons pas : la potentialité existe et ce n'est pas parce que vos données sont peu exploitées en public qu'elles ne sont pas exploitées par les entreprises concurrentes.
- La seconde qui est un peu la conséquence de la première, c'est que définir ce qui doit être public –souvent vous ne déciderez pas de manière autonome mais devrez suivre les lois, les règles de la CNIL, les usages etc...- va permettre de définir, négativement en quelque sorte, tout ce qui n'est pas données publiques et donc doit rester à l'intérieur de l'organisation et être protégé.

C'est un travail conséquent à faire, mais l'enjeu est encore plus important. Définir dans une organisation tout ce qui doit être public et ce qui ne l'est pas, c'est faire progresser la culture du management de l'information et favoriser la gestion dynamique du « record », de l'archivage.