arbido

2016/3 Détruire pour conserver?

Fuentes Hashimoto Lourdes, chef du service des archives électroniques, Groupe Total

Gérer le cycle de vie de l'information pour maîtriser les risques juridiques et financiers: le discovery

Face aux procédures judiciaires américaines de *discovery*, l'évaluation archivistique se pose en termes différents pour les organisations qui risquent d'y être confrontées. La surconservation des données qui ne sont plus nécessaires aux activités de l'organisation présente un double risque: risque de communiquer des informations stratégiques qui peuvent porter atteinte à son action et à son image et risque de divulguer massivement des données susceptibles de porter atteinte aux droits des personnes.

Respect du cycle de vie et réglementations

L'identification des documents produits par une organisation – publique, parapublique ou privée – dans l'exercice de ses activités, l'attribution d'une durée de conservation à chaque typologie documentaire ainsi que l'association d'un sort final – destruction ou conservation définitive – lorsque la durée de conservation arrive à échéance constituent le pilier de la gestion documentaire (ou records management) et de l'archivage.

Cette pratique que les records managers ou archivistes appellent communément «gestion du cycle de vie de l'information» est au cœur d'une bonne politique de gouvernance de l'information: elle permet de maîtriser dans la durée l'ensemble des documents utiles à une organisation pour des raisons juridiques, stratégiques et/ou patrimoniales. La gestion du cycle de vie de l'information, quel que soit son support, est fondamentale pour éviter à la fois la destruction inopinée de documents ayant encore une utilité, la dispersion de l'information confidentielle, la surconservation génératrice de coûts et de pertes de productivité et pour garantir la constitution du patrimoine informationnel. L'attribution des durées de conservation s'opère en fonction du cadre réglementaire et juridique applicable aux activités de l'organisation. Ce cadre peut être plus ou moins contraignant et complexe: il est impératif de respecter de nombreuses règles propres au pays où l'activité est exercée ainsi que la réglementation européenne, le cas échéant.

Toutes les organisations exerçant leur activité aux États-Unis, par exemple via des filiales implantées sur le territoire américain, ou ayant des liens commerciaux avec ce pays, sont soumises également aux injonctions de la justice américaine, en particulier à la procédure dite de *«discovery»*. L'obligation de répondre à ces injonctions renforce la nécessité de contrôler davantage l'information. La gestion de son cycle de vie est incontournable. En quoi consiste exactement le *discovery*? Et quels sont les enjeux en termes de gouvernance de l'information?

Les procédures de discovery

Le *discovery* est une procédure en droit civil fédéral américain *(federal rules of civil procedure).* Elle s'applique en amont d'un procès pour permettre la constitution du dossier de chacune des parties qui a donc le droit de demander des dossiers/documents à l'autre, voire d'intervenir directement à la recherche de tout élément pouvant conduire «raisonnablement à une preuve ou évidence recevable par la justice» selon les termes de la loi américaine. Ainsi, chaque partie est libre de réunir tous les éléments qui permettent de constituer le dossier qui sera présenté au tribunal pour attaquer l'autre partie dans le cadre d'un contentieux.

La recherche d'éléments pouvant constituer une preuve ouvre la voie à une recherche documentaire très élargie qui peut être qualifiée d'intrusive en raison de son caractère soudain et contraignant. Il convient de noter que si une partie prend la décision de ne pas communiquer des informations, son refus pourra être utilisé contre elle. Elle encourt alors des sanctions. Toutes les parties ont donc intérêt à jouer le jeu en autorisant la recherche documentaire et en livrant tout élément réclamé par la partie adverse. Toute information dissimulée qui serait découverte a posteriori risque de porter atteinte à la partie, voire de lui faire perdre le procès.

Le terme d'*«e-discovery»* est utilisé lorsque l'on se réfère à des documents mobilisés dans les procédures de *discovery* qui sont sous forme électronique (données applicatives, logs, documents électroniques sous différents formats, etc.).

Certains types de document sont exclus de la procédure car ils sont considérés comme étant «protégés». Les données personnelles peuvent dans certains cas être concernées par cette protection. Cependant, celle-ci dépend entièrement du type de procès.
Par conséquent, des données personnelles sont susceptibles d'être sollicitées. Cela implique une vigilance accrue pour ne pas porter atteinte aux droits des personnes.

Dans la justice américaine, les procédures de *discovery* permettant de constituer les dossiers en amont du procès conduisent généralement à des accords entre les parties qui sont libres de décider ensuite si elles vont, ou non, au tribunal. Ainsi, bon nombre de contentieux sont réglés par des accords et ne donnent pas lieu à des procès.

La procédure de *discovery* peut se traduire par des demandes formelles d'information (*roquets for production of documents*), des recherches directes d'information par l'intermédiaire de tiers (comme un moniteur par exemple), des dépositions, des interrogatoires, etc. La plupart des États américains ont adhéré au *Uniform Interstate Depositions and Discovery Act* et appliquent donc la loi fédérale en matière de *discovery* avec toutefois quelques exceptions. Au Royaume-Uni, la procédure de *discovery* est plutôt connue sous le nom de *«disclosure».*

Le *discovery* existe depuis la fin des années 1940, mais il a été renforcé de manière significative en 2006 lorsqu'il a été manifestement élargi à toutes les informations électroniques incluant notamment les logs de connexion et les mails du personnel. Par conséquent, les procédures de *discovery* et d'*e-discovery* conduisent à d'importants transferts de données vers les États-Unis à la demande de juridictions américaines. Pour cette raison, en France, la Commission Nationale Informatiques et Libertés (CNIL) s'est saisi de la problématique [12].en 2007–2009 et le G29 en 2009. La CNIL a émis la délibération n°2009–474 «portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de Discovery ». Elle rappelle la nécessité de s'assurer de la légitimité et de la finalité des traitements d'information opérés dans le cadre du *discovery*.

Discovery et respect des droits des personnes

Le respect des conventions internationales et des dispositions nationales applicables, telles que la Convention de La Haye et la loi du 26 juillet 1968, est nécessaire afin de protéger les droits fondamentaux des personnes concernées. La CNIL a rappelé que la législation américaine diffère de celle appliquée en Europe en matière de protection des données personnelles. Les transferts de données doivent être déclarés à la CNIL.

Le G29, groupe de travail européen,a demandé le respect d'un principe de proportionnalité dans le cadre de «procédures civiles transfrontalières» afin de ne pas divulguer des informations non requises pour le procès en question. Il préconise une coordination internationale menée par les gouvernements des États concernés, éventuellement par l'adoption d'un traité ou d'une convention (avis du 11 février 2009[345]

Les entreprises américaines sont tenues de certifier le respect de conventions européennes afin d'obtenir le transfert de données personnelles. Les États-Unis ont mis en place un cadre spécifique appelé Safe Harbor. En concertation avec la Suisse, il existe un «US-Swiss Safe Harbor Framework». Toutefois, les accords du Safe Harbor ont été invalidés en 2015 par la Cour de justice de l'Union européenne, sujet qui a fait la une des journaux spécialisés. Les liens entre le discovery et la protection des données personnelles sont donc épineux.

Nécessité de maîtriser l'information dès sa production

Le *discovery* et l'*e-discovery* sont des procédures intrusives, coûteuses en temps et en argent et difficiles à maîtriser s'il n'y a pas de réflexion en amont pour être en mesure de répondre efficacement, sans compromettre les droits des personnes, aux injonctions de la justice américaine.

En France, toute organisation soumise à ces procédures doit s'assurer par ailleurs du respect des recommandations de la CNIL. Elle doit répondre à toutes les demandes d'information dans le cadre d'un contentieux en lien avec la justice américaine, permettre la recherche directe en ouvrant l'accès à l'information à son opposant, recherche qui se traduit dans bien des cas par l'accueil d'un moniteur qui investigue sur place. Les informations conservées par une partie qui sont exigées par l'autre partie peuvent être soumises à un gel à la destruction et/ou à la com-munication. Autrement dit,

1. il est demandé d'interrompre l'application du cycle de vie tel que défini dans la politique de gestion docu-mentaire de l'organisation lorsqu'elle existe et
2. il est exigé que certains documents ne soient plus consultés par d'autres interlocuteurs pendant une période qui peut être plus ou moins longue en fonction des contentieux

La fourniture d'informations et la gestion des gels nécessitent une organisation appropriée qui se traduit notamment par la mise en place des procédures et des modes opératoires clairs et validés par les responsables juridiques (la direction juridique lorsqu'elle existe). En effet, le temps nécessaire pour mettre la main sur les informations demandées peut être assez long si les informations sont éparpillées ou bien si on ignore où se trouve cette information. Dès lors, les impacts en termes de gestion de l'information sont importants.

Toute organisation susceptible d'être engagée dans une procédure de *discovery* se doit de maîtriser l'information qu'elle produit, elle doit être en mesure de prouver que la destruction de documents, si elle a eu lieu, a été effectuée conformément à une politique interne reconnue pouvant être auditée. C'est ainsi que des politiques de gouvernance de l'information se sont développées dans la plupart des entreprises multinationales dans le monde. Elles se sont dotées de politiques internes permettant de garantir la conformité aux règles de protection des données personnelles et la mise en œuvre de politiques d'archivage appropriées au contexte local, européen et américain.

Trop conserver, une pratique à risque

La gestion du cycle de vie de l'information devient donc un enjeu majeur pour la maîtrise des risques financiers et juridiques: il s'agit de maîtriser l'information qu'on produit, de bien gérer en conséquence son cycle de vie, c'est-à-dire de conserver et de détruire ce qui doit être conservé ou détruit en fonction de la réglementation en vigueur.

Ce contexte favorise également la mise en place de politiques d'archivage électronique qui permettent de bien contrôler l'information sous forme électronique: l'identifier, la répartir en catégories, lui attribuer des durées de conservation et un sort final. Toute organisation doit savoir où se trouvent ses données et qui peut y avoir accès.

La surconservation des données électroniques qui ne sont plus nécessaires aux activités de l'organisation présente un risque qui est double: le risque de communiquer de manière élargie des informations stratégiques à un secteur d'activité qui peuvent porter atteinte à son action et à son image et le risque de divulguer massivement des données susceptibles de porter atteinte aux droits des personnes.

1 https://www.cnil.fr/fr/quel-ca

2 En ligne. Consulté le 30 juin 2016

3 <

4 http://ec.europa.eu/justice/po...

5 privacy/docs/wpdocs/2009/wp158_fr.pdf> En ligne. Consulté le 30 juin 2016.

Lourdes Fuentes Hashimoto

Lourdes Fuentes Hashimoto est une archiviste franco-mexicaine spécialisée dans la conception, l'audit et le pilotage des systèmes d'information pour la gestion des archives, tous supports confondus, et la conduite de projets d'archivage électronique dont les interfaçages entre les applications métier et les systèmes d'archivage électronique. Elle a conduit plusieurs projets informatiques depuis plus de sept ans. Elle travaille, depuis 2013, au sein du Groupe Total où elle a dirigé le projet e-TRACES de refonte et de migration du système d'archivage électronique. Le système est en production depuis le mois d'avril 2016 et sera interfacé fin 2016 avec plusieurs applications. Il est ouvert aux collaborateurs du groupe dans le monde (130 pays) et permet de conserver les documents dès leur validation et pendant tout leur cycle de vie, y compris pour conservation définitive. Auparavant, elle a exercé des missions similaires au ministère français des Affaires étrangères et au conseil général de la Seine-Saint-Denis.

Résumé

Deutsch

Der Dokumentenzyklus will gemanagt sein, um juristische und finanzielle Risiken zu bewältigen: Discovery-Verfahren

Immer komplexere Regelungen, die dazu tendieren, den lokalen, europäischen und amerikanischen Kontext zu überdecken, machen für Organisationen die Beherrschung der produzierten Informationen für die Ausübung ihrer Aktivitäten erforderlich. Ein umfassendes Life Cycle Management von Information, das heisst das Identifizieren der verschiedenen Arten von Dokumenten, die produziert werden – Festlegung der Aufbe-wahrungsfristen von Fall zu Fall sowie endgültige Sortierung (Vernichtung oder Aufbe-wahrung) – ist unumgänglich für Organisationen, die mit zahlreichen Anträgen von verschiedenen Gerichtsbarkeiten, einschliesslich amerikanischer, konfrontiert werden. Im Fall einer Rechtsstreitigkeit kann die amerikanische Justiz aufgrund sogenannter Discovery-Verfahren von einer Organisation die Lieferung zahlreicher physischer oder elektronischer Informationen verlangen. Bei elektronischen Daten spricht man deshalb auch von E-Discovery. Jede Organisation, die in den oder mit den Vereinigten Staaten tätig ist, kann jederzeit in Verfahren solcher Art involviert werden. Durch die Offenlegung von Informationen kann ihre Tätigkeit durch die Konkurrenz beeinträchtigt werden. Oder sie könnte im Fall einer Verbreitung von persönlichen Daten die Rechte von Personen kompromittieren. Eine Organisation ist daher verpflichtet, ihre Bemühungen für die Beherrschung des Informationsmanagements sowie der rechtlichen und finanziellen Risiken zu erhöhen.