PÉRENNITÉ ET CONSERVATION DES ACTES DE L'ÉTAT CIVIL

Françoise BANAT-BERGER

Direction des archives de France

Le contexte. Les actes authentiques électroniques et l'archivage

C'est lors des discussions au Parlement relatives au vote de la future loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatives à la signature électronique, que la question de la conservation pérenne des actes a été abordée[1]. Le principe du projet de loi était d'accorder la même valeur de preuve aux écrits sur support numérique qu'aux écrits sur support papier, à condition que l'identification des auteurs des actes soit assurée et que les actes soient établis et conservés de manière à en garantir l'intégrité[2]. Or, au-delà de cette importante innovation, un amendement a été introduit visant à permettre que les actes authentiques électroniques puissent également être établis sous forme électronique[3]. Il s'agit des actes dont la valeur de preuve est la plus forte dans le droit français[4]. On remarque à cet égard qu'une importance toute particulière a été accordée à la signature électronique puisque désormais c'est la signature qui confère l'authenticité à l'acte. Concernant ces actes, un décret était prévu afin de préciser les conditions dans lesquelles l'authenticité et la pérennité des actes électroniques seront garanties.

La question de la conservation est abordée car les parlementaires ont conscience lorsqu'ils évoquent les actes authentiques que ces derniers doivent être conservés durant une longue période. En fait, il s'agit d'une conservation pour une durée illimitée qui est assurée par les services départementaux d'archives.

On a ainsi pu entendre M. Vaillant alors ministre des relations avec le Parlement, reconnaître que :

> "*Les techniques actuelles ne permettent de garantir la conservation des informations que pour une durée limitée en raison de leur obsolescence rapide. Il est certes possible de faire passer les informations d'un support à un autre au fur et à mesure des évolutions, mais la récupération de l'information devra être sécurisée. Les conditions techniques d'une dématérialisation des actes authentiques ne sont donc pas réunies"* et qu' *"au total, le Gouvernement accepte l'idée d'inscrire le principe de la dématérialisation dans le Code civil, tout en renvoyant à plus tard les conditions matérielles de sa réalisation*"

Malgré cette mise en garde, deux décrets sont mis assez rapidement en préparation concernant les actes des notaires et des huissiers. Il a toutefois fallu attendre plusieurs années (août 2005) pour que ces textes soient publiés[5] en raison notamment de problématiques liées à la conservation pérenne : d'une part la problématique des migrations de format, d'autre part, celle du maintien à long terme des signatures électroniques et enfin plus généralement la complexité et coût de la conservation numérique sur le long terme[6].

A cet égard, plusieurs réponses sont apportées dans ces décrets qui, ainsi, intègrent la notion de métadonnées, à savoir l'enregistrement et la traçabilité des éléments descriptifs et de structure, mais également de gestion et techniques, permettant de retrouver, identifier et caractériser aisément les actes. De même, la complexité de l'archivage électronique a justifié le choix de mettre en œuvre un minutier central électronique par profession, les notaires et les huissiers transmettant les actes élaborés rapidement après leur production et confiant leur conservation à cette structure centrale.

Enfin, pour la première fois, a été soulevée la contradiction visant d'une part, à maintenir l'intégrité des actes au sens technique du terme (bit par bit) ; et d'autre part, le maintien de la lisibilité sur le moyen et le long terme des actes, qui implique notamment de procéder à des migrations de format qui modifient l'acte et, par conséquent, invalident le procédé de vérification de signature (l'intégrité bit par bit ne peut plus être assurée)[7]. Cette contradiction insoluble, dès lors qu'on fait reposer la sécurité juridique d'un acte sur un procédé technologique, a été écartée dans les décrets, par une parade juridique visant à poser le fait que les migrations nécessaires à assurer la lisibilité de l'acte, ne lui retirent pas son caractère d'original.

---

1. Consulter pour davantage de précisions l'article suivant : BLANCHETTE, Jean-François et Françoise BANAT-BERGER. 2006. La "dématérialisation" des actes authentiques en droit français. Gazette des Archives, Association des archivistes français, n°204.
2. ..."*sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité*." (CC, art.1316-1)
3. "*Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat* ". (CC, art.1317)
4. Minutes des notaires et des huissiers de justice, minutes judiciaires et actes d'état civil.
5. Décrets n° 2005-972 et 973 du 10 août 2005, relatifs respectivement aux actes authentiques des huissiers et des notaires.
6. Il a fallu attendre encore quelques années pour que le minutier central des notaires soit inauguré le 28 octobre 2008 et refermé tout aussitôt en attendant sa mise en œuvre effective.
7. Voir BLANCHETTE, Jean-François et Anne CANTEAUT. 2007. Intégrité, signature et processus d'archivage. In *La sécurité aujourd'hui dans la société de l'information*, sous la dir. de Stéphanie Lacour. L'Harmattan.

Les actes de l'état civil et leur archivage

La situation actuelle

Concernant les actes de l'état civil, la tenue d'un double original sur papier est actuellement toujours exigée[8]. Cependant, depuis 1989, le double déposé au greffe du tribunal n'est plus tenu à jour. On assiste depuis quelques années à une centralisation des nouveaux actes de naissance, 90% du flux traité par un peu plus de 700 mairies, ainsi qu'une utilisation massive depuis 1998 de logiciels métiers d'état civil, plus de 7000 mairies sont aujourd'hui informatisées dont la totalité des mairies de plus de 8000 habitants. Dans de nombreux cas également, les registres papier encore conservés à la mairie ont fait l'objet en totalité ou en partie d'une intégration dans la base de données (soit sous forme image après numérisation des actes ou après une re-saisie en mode texte). Toutefois, le registre numérique n'a aucune valeur probante, la valeur probante reposant uniquement sur les registres papier.

C'est ainsi que, dans les mairies informatisées, les actes sont établis et mis à jour sous forme numérique tandis que les registres papier sont édités à partir du logiciel métier, l'officier d'état civil apposant sa signature manuscrite sur chaque acte ainsi établi. Il y a manipulation du registre papier communal dans la mesure où les mises à jour doivent être portées sur ce registre papier et signées d'une manière manuscrite également. Seul le service central d'état civil de Nantes[9] ne tient plus à jour que son registre numérique mais, nous y reviendrons, le service de Nantes est un service centralisé. Les échanges d'informations entre mairies, mairies et notaires s'effectuent toujours sous forme courrier, à l'exception de quelques expérimentations de transmissions électroniques[10]. Le système est par conséquent relativement lourd, d'autant qu'on assiste à une augmentation importante du nombre de mentions marginales en raison de la mobilité familiale de plus en plus importante des personnes. La double tenue papier/numérique est par conséquent parfois complexe à assurer et peut engendrer des discordances en ce qui concerne l'actualisation des deux supports. De même, les échanges d'information en raison de la dispersion géographique des actes sont de plus en plus importants, ce qui rend les échanges traditionnels par envois postaux de plus en plus coûteux.

La dématérialisation des actes en utilisant des outils de signature électronique semble évidente et aller dans le sens d'une plus grande efficacité et simplicité en suivant l'exemple des notaires et des huissiers. Et pourtant, cela n'est pas si simple.

Vers la dématérialisation ?

Dans un premier temps, la réflexion a porté sur la constitution d'un registre national de l'état civil, à l'instar de ce qui a été décidé pour les notaires et huissiers et de ce qui a été réalisé dans d'autres pays comme la Suisse ou l'Ecosse. L'avantage est évident de disposer ainsi d'un service fiable notamment pour les mises à jour, à même d assurer une véritable sécurité technique en mutualisant les coûts liés à la conservation numérique sur le long terme. Ceci étant, pour l'instant, l'hypothèse a été écartée pour de nombreuses raisons. Raisons de coût[11], bien évidemment avec des interrogations sur la structure qui assurerait cette mission, incertitudes sur l'environnement technique et juridique avec les interrogations légitimes du point de vue de la législation sur les données à caractère personnel, que ne manquerait pas de poser la constitution d'un grand "registre central de la population". Enfin, la dimension symbolique du changement est extrêmement importante, avec l'impression de dessaisissement que pourraient ressentir les communes quant à leurs missions traditionnelles.

Une autre piste a alors été évoquée : donner une force probante au registre numérique et n'exiger que la tenue d'un seul registre papier qui ne serait plus tenu à jour. Plusieurs scénarii seraient envisageables selon que la commune serait ou non informatisée : registre papier et registre numérisé dans un cas[12] ; registre numérique avec la mise en œuvre de signatures électroniques et registre papier dans le second cas. Ne seraient alors déposées aux greffes des tribunaux que les copies numériques. Il s'agit d'une solution apparemment simple et pragmatique[13] mais sans que les problématiques de conservation pérenne soient évoquées. Toutefois, des questions de base ne sont pas traitées. Ainsi concernant la copie numérisée d'un original papier pour une commune non informatisée : comment sera-t-il possible, avec une simple gestion électronique de documents (GED), sans application métier, de gérer les mises à jour d'actes scannés à une date donnée ?

Les questions relatives à la signature électronique

Par ailleurs, concernant les actes établis nativement sous forme numérique et dotés d'une signature

8. Décret n° 62-921 du 3 août 1962 modifiant certaines règles relatives aux actes de l'état civil.
9. Pour les français nés à l'étranger.
10. Par exemple, le département des Deux-Sèvres est pilote de la dématérialisation des demandes de validation d'informations d'état civil entre organismes sociaux et collectivités. Un projet de décret concerne également la dématérialisation des transmissions entre le service de l'état civil de Nantes et ses partenaires (professionnels : notaires, caisses de retraite...), communes.
11. Les pays assurant une conservation centralisée de l'état civil sont de plus petits pays, qui dans certains cas s'appuient sur une tradition de centralisation multiséculaire, dans d'autres cas n'ont pas la même réglementation qu'en France, notamment concernant les mises à jour.
12. Sans signature électronique dans ce cas.
13. Avec des économies de stockage de la collection papier du greffe évidentes.

électronique : quid des signatures des mises à jour? quid du maintien sur le long terme de la vérification technique des signatures, une fois les durées des certificats expirés (au bout de trois ans au maximum) ? Ceci nécessite d'expliquer en quelques lignes la technologie mise en œuvre pour les signatures électroniques telle qu'elle est définie par le décret n°2001-272 du 30 mars 2001 en application de la loi du 13 mars 2000.

Les technologies de signature électronique

Le système repose sur trois éléments : la génération d'une empreinte[14], la signature de l'empreinte avec une clé privée (secrète) et l'établissement du lien entre la clé privée et son propriétaire. L'empreinte de taille généralement fixe, est générée à partir du document dont on souhaite prouver l'intégrité, grâce à une fonction mathématique dite fonction de hachage. Cette fonction restitue une empreinte indissociable du document dont elle est extraite et qui est d'une longueur fixe. L'empreinte est transmise avec le document et à l'arrivée, avec la même fonction, le système prend une empreinte du document reçu et compare les deux empreintes. Si le résultat est identique, cela signifie qu'une probabilité très élevée existe qu'il n'y a pas eu d'altération du document durant la transmission.

Toutefois, durant la transmission, le document et son empreinte auraient pu être subtilisés et remplacés par un autre document avec sa propre empreinte. C'est la raison pour laquelle l'empreinte de départ est signée avec la clé privée (secrète) de son auteur et l'empreinte générée à l'arrivée est vérifiée avec la clé publique correspondant à la clé privée, et qui elle, est destinée à être communiquée à quiconque veut vérifier la signature. Ainsi, si l'empreinte permet de s'assurer qu'un document n'a pas été altéré, la signature permet en plus de certifier la provenance du document. On parle alors de "non-répudiation": l'auteur ne peut pas ne pas reconnaître être l'auteur de l'acte dans la mesure où la clé publique ne peut vérifier positivement que ce qui a été signé par la clé privée correspondante.

Enfin, il reste à s'assurer du lien entre la clé privée et son propriétaire. C'est là qu'interviennent les prestataires de certification auprès desquels on va faire enregistrer sa clé publique. Ainsi un tiers (le prestataire) se porte garant que la clé publique est bien la vôtre et de la sorte, est créé un lien entre la clé publique et votre identité. L'enregistrement se fait sur un certificat qui contient un certain nombre d'informations variable suivant les niveaux de sécurité : identité de son propriétaire, qualité, clé publique…

Deux éléments très importants sont ainsi, d'une part, la durée de validité du certificat (généralement entre un et trois ans) et, d'autre part, les transactions qui sont permises pour ce certificat. Bien évidemment, le certificat est à son tour signé avec la clé privée du prestataire. Ce système relativement complexe induit la mise en place d'une infrastructure, et on voit que la vérification d'une signature implique la conservation, parallèlement au document proprement dit, notamment des algorithmes de signature utilisés au moment où le document a été signé, ainsi que celle des certificats (on doit s'appuyer sur celui qui était valide au moment où le document a été signé).

Le maintien sur le long terme de la signature électronique

Dans ces conditions, comment maintenir sur le long terme la possibilité de vérification de la signature électronique, sur laquelle repose tout le système puisque l'authenticité de l'acte repose sur sa signature ? Faut-il resigner à l'expiration des durées de vie des certificats[15], l'ensemble des actes par certificat serveur pour une masse qui ne fera que s'accroître d'année en année ? Le coût et la lourdeur de la solution sont évidents. Ne faut-il pas préférer une adaptation juridique qui permette de s'abstraire de cette lourdeur, par exemple en imaginant la production d'une attestation au moment de la vérification "originelle" de l'acte permettant de s'assurer que telle signature, portant sur tel acte, était bien valide à telle date et qu'ensuite le maintien de son intégrité repose sur le processus d'archivage ?

Les questions relatives aux formats d'encodage des actes

Le format peut être défini comme l'ensemble des caractéristiques logiques d'organisation de l'information : c'est ce que l'on appelle le format de données, le format de fichier ou encore le format de représentation de l'information. Or, il existe différentes manières de représenter l'information sous forme binaire. Les trains de bits, mêmes regroupés en mots binaires, n'ont aucune signification pour un humain. L'interprétation des mots binaires en informations compréhensibles est réalisée par des programmes informatiques appelés aussi logiciels. Il en existe une quantité presque innombrable remplissant chacun différentes fonctions à différents niveaux. Ces programmes doivent disposer d'une connaissance complète de la manière dont l'information est organisée au sein des structures binaires.

Dans le travail quotidien, les agents utilisent des formats texte dits bureautiques (formats de la suite Office, formats de la suite OpenOffice, format texte..), ou encore des formats images. La difficulté intrinsèque est qu'aujourd'hui beaucoup d'agents travaillent avec des formats qu'on appelle "fermés", c'est à dire dont les spécifications ne sont pas publiques. Par exemple, si un document a été produit au format Word 97, son ouverture est liée au logiciel de la société Microsoft qui permet de l'interpréter ainsi qu'au système

14. On utilise également les termes de condensat ou digest (anglais) pour désigner l'empreinte. La fonction de hachage (ou hash en anglais) est la fonction permettant le calcul de l'empreinte.
15. Au maximum tous les trois ans.

d'exploitation adéquat (Windows XP, ou Vista). Aujourd'hui, si un agent dispose de la suite office 2007, il ne pourra plus ouvrir des fichiers Word 97 et ne disposera pas des spécifications du logiciel permettant d'interpréter les fichiers ainsi produits. La chaîne de compatibilité est ainsi rompue en moins de 10 ans. En effet, si les éditeurs généralement permettent une compatibilité ascendante par exemple entre une version N et une version N+1, celle-ci ne sera plus assurée lors du passage à la version suivante.

A l'inverse, les formats édités par la société Adobe[16] sont propriétaires dans la mesure où ils appartiennent à la société Adobe qui peut évidemment changer de politique commerciale. Toutefois cette société a toujours fait le choix de publier les spécifications de ses formats, ce qui signifie que lorsqu'on souhaite ouvrir un fichier produit à partir d'une version ancienne de PDF, il sera toujours possible d'écrire un programme permettant d'interpréter correctement ce fichier à partir des spécifications de cet ancien format qui sont publiques.

Il est par conséquent essentiel, pour des documents que l'on souhaite conserver sur le moyen et long terme, de faire le choix de formats ouverts, dont la documentation est complète et accessible à tous, qui reposent si possible sur des normes ou standards[17]. Ces formats doivent autant que possible être indépendants vis-à-vis des autres formats, vis-à-vis des plateformes (systèmes d'exploitation), ainsi qu'au plan économique (coûts de développement des outils de manipulation raisonnables). Les formats simples sont préférables aux formats complexes.

Si dès la production pour les actes de l'état civil, les formats utilisés ne correspondent pas à ces critères, des migrations vers des formats pérennes seront à mettre en œuvre le plus rapidement possible, ce qui bien évidemment invalidera les processus de vérification des signatures électroniques. Si dès l'origine des formats pérennes sont choisis, ces migrations seront repoussées dans le temps, mais devront cependant à long terme intervenir. En effet, il est impossible de concevoir qu'un format reste stable sans évolution durant plusieurs dizaines d'années. Il conviendra par conséquent de le prévoir afin d'assurer une force juridique aux actes ainsi migrés. Les décrets relatifs aux notaires et huissiers ont ainsi permis que les migrations nécessaires à la lisibilité des actes ne retirent pas à ces derniers leur caractère d'original. Plus largement, cette conception rejoint la recommandation en date du 1er décembre 2005 du forum des droits sur internet (FDI)[18] relative à la conservation numérique. En effet, la recommandation définit ce qu'on doit entendre par "intégrité", afin d'interpréter l'article 1316-1 du Code civil : cette notion serait assurée en fait, par le respect cumulé des trois critères que sont la lisibilité du document, la stabilité du contenu informationnel et la traçabilité des opérations sur le document.

Les questions relatives à la conservation sécurisée

Très généralement les organisations qui envisagent de dématérialiser un processus évoquent les économies réalisées en termes de locaux d'archivage traditionnels. Ces économies sont évidemment réelles, mais il est frappant que, parallèlement, ne soit absolument pas évalué le coût de la conservation numérique en termes cette fois de compétences, de matériels et de logiciels.

Une politique d'archivage

D'une manière générale, la mise en œuvre d'un archivage sécurisé sur le long terme nécessite l'adoption d'une politique d'archivage, sur le modèle de celle élaborée en 2006 par la direction centrale de la sécurité des systèmes d'information[19]. L'archivage électronique, objet de cette politique d'archivage type (PA), vise ainsi à conserver l'information en la restituant de manière intègre et conforme à l'information d'origine. Cette opération de conservation des archives ayant une force probante et des effets juridiques concerne toutes les personnes juridiques sans exception, qu'elles soient physiques, morales, privées ou publiques.

L'élaboration de la politique d'archivage passe en premier lieu par la détermination des responsabilités et obligations entre les différents acteurs, par exemple entre le service producteur, le service informatique et le service d'archives. Seront notamment définies les autorités d'archivage, l'autorité d'archivage étant celle qui a la responsabilité de l'archivage en charge de la gestion, du traitement, de la conservation et de la communication des données.

Sont ainsi définies les exigences minimales, en termes juridiques, fonctionnels, opérationnels, techniques et de sécurité, qu'une autorité d'archivage doit respecter afin que l'archivage électronique mis en place puisse être regardé comme fiable.

16. Les formats PDF.
17. Pour les fichiers bureautiques, format ODF (open document format) diffusé par exemple par la suite open office (norme ISO 26300, 2006) ; version 1.7 de PDF qui est devenue la norme ISO 32000-1 2008 ; format d'archivage PDF/A-1 (norme ISO 19005-1 : Electronic Document file format for long-term preservation). Pour les formats images : formats TIFF, JPEG (norme ISO/IEC IS 10918-1), JPEG2000 (norme ISO/IEC -15444), PNG (norme ISO/IEC 15948:2003). Pour les langages, format XML, version 1.0, qui est standardisé par le W3C (World Wide Web Consortium).
18. FORUM DES DROITS SUR L'INTERNET (FDI). 2005. Conservation électronique des documents. La recommandation est publiée à l'adresse suivante : http://www.foruminternet.org/activites_evenements/lire.phtml?id=126
19. DIRECTION DE LA SECURITE DES SYSTEMES D'INFORMATION (DCSSI). 2006. Outils méthodologiques pour la sécurité des systèmes d'information. Archivage électronique sécurisé http://www.ssi.gouv.fr/fr/confiance/archivage.html.

La nécessité d'un stockage sécurisé

La sécurisation du stockage doit bien évidemment être assurée quel que soit le type de support choisi (support en ligne : disques, supports à accès différé : cartouches, bandes, supports optiques amovibles..). Le choix dépendra des besoins en type de rapidité d'accès, de besoins en termes de nombre de consultations. Mais quel que soit le choix effectué, il est essentiel de mettre en œuvre une surveillance des supports (manuelle mais si possible automatisée) afin de pouvoir réaliser si nécessaire des migrations de supports. Il faudra également décider du renouvellement au bout d'un délai à fixer suivant le type de support, de ces supports[20]. Ceci implique de mettre en œuvre des procédures, de disposer de métadonnées techniques suffisantes pour réaliser une surveillance sur des échantillons représentatifs, ainsi que de connaissances suffisantes sur les supports et leur qualité[21]. Dans tous les cas, également, il faudra pour des raisons évidentes de sécurité des données[22], au-delà des technologies de redondance, assurer la duplication des informations sur deux sites distants.

Les autres coûts associés

Au-delà de ces coûts, devront être intégrés, nous l'avons dit, les coûts liés à la migration des formats (mise en œuvre d'outils de reconnaissance et validité des formats entrants et stockés, outils de conversion avec traçabilité rigoureuse des opérations et conservation des formats d'origine) ; aux dispositifs relatifs à la sécurisation des actes conservés (technologies relatives aux empreintes et à l'horodatage du processus d'archivage : il faut pouvoir prouver que telle opération a été effectuée à telle date, et il faut pouvoir prouver que les actes conservés sont restés intègres depuis leur établissement); aux transmissions par exemple pour archivage définitif dans les services publics d'archives : export des données au format du standard d'échange de données pour l'archivage[23] à mettre en œuvre, sans compter les coûts relatifs aux fonctionnalités de recherche et de consultation avec les habilitations associées.

Conclusions

On le voit, l'archivage numérique induit une complexité, des compétences et des coûts importants. Qui, dans le cas des actes d'état civil numériques, doit supporter ces charges et quelle doit être l'organisation à mettre en place ?La mutualisation est une source évidente d'économie et de sécurité à la fois, mais implique des coûts initiaux importants (service central) et des problèmes juridiques importants. Cette solution a été écartée pour l'instant.

Ainsi, si l'on garde l'organisation actuellement en place, la responsabilité et le coût reposeraient sur les communes et les greffes des tribunaux dont les agents actuellement n'ont ni le profil ni les compétences nécessaires à cette conservation numérique sur le long terme. Celle-ci serait ensuite prise en charge par les services départementaux d'archives mais au terme d'un délai qui, aujourd'hui, est de cent ans...

Le plus dangereux est de ne pas évoquer ces questions et ainsi de mettre en œuvre la dématérialisation sans se donner les moyens d'une conservation sécurisée des données numériques soit en pensant avoir une sécurité liée à une simple technologie de signature électronique elle-même peu pérenne, soit en pensant avoir une sécurité en gardant par exemple un original papier mais qui ne serait plus mis à jour alors même que les données numériques ne sont pas sécurisées quant à leur conservation sur le long terme. Par conséquent, on ne peut pas se permettre d'improviser en se "contentant" d'une sécurité juridique apportée par un décret pour les actes fondamentaux de l'état et du droit des personnes. On doit à la fois mettre en œuvre une sécurité juridique, technique, archivistique, faute de quoi on aura joué aux apprentis sorciers et on aura permis une régression de plusieurs centaines d'années quant à la conservation de l'état civil des personnes.

20. Par exemple si on utilise des bandes, décider de migrer systématiquement l'ensemble des actes au bout de 5 ans et chaque année, dérouler chaque bande.

21. Ainsi, pour les CD-R et les DVD-R, ce sont deux études scientifiques confiées par la direction des Archives de France au laboratoire national de métrologie et d'essais (LNE) qui ont permis de définir des marques de CD ou de DVD associées à des types de graveurs, susceptibles d'avoir une véritable qualité dite "d'archivage", sans se reposer sur les assertions des fabricants (Instruction DITN/RES/2005/004 du 29 mars 2005 relative à la gravure, à la conservation et à l'évaluation des CD-R. Instruction DITN/RES/2006/003 du 20 décembre 2006 relative aux résultats de l'étude sur les CD-R conservés par les services publics d'archives. Note d'information DITN/RES/2008/012 du 19 décembre 2008 relative aux résultats d'une seconde étude sur des CD-R et des graveurs du marché, ainsi que d'une étude sur les DVD-R et graveurs du marché : http://www. archivesdefrance.culture.gouv .fr/gerer/archives-electroniques/stockage/

22. Une étude réalisée par Google (en fait des statistiques s'appuyant sur l'observation continue pendant plusieurs mois de 100 000 disques durs de marques, de capacités et de vitesses de rotation variées, disques utilisés par Google dans ses locaux de Mountain View, en Californie) fait ressortir, d'une part, un risque de "mort subite" du disque dur neuf (le taux de panne est près de deux fois plus élevé chez les disques de moins de trois mois, que chez ceux de plus d'un an), d'autre part, un taux de panne qui augmente rapidement : pendant la première année d'utilisation, seuls 1,7 % des 100 000 disques durs de Google ont dû être remplacés, puis 8 % au cours de la deuxième année, 8,6 % la troisième.... et enfin une relative inefficacité des alertes existantes : 56 % des disques durs qui ont rendu l'âme l'ont fait sans qu'il y ait eu d'alerte. Par ailleurs, il semble que les disques soient de plus en plus fragiles à mesure que leur capacité augmente.

23. Il s'agit du format d'échange de données pour l'archivage publié en 2006 par la DAF et la direction générale de la modernisation de l'Etat (DGME) pour les services d'archives et leurs partenaires (notamment les producteurs d'archives). Ce format spécifie la structure et le contenu des messages produits dans le cadre de ces transmissions, ainsi que le contenu des bordereaux de versement qui sont transférés en même temps que les actes à archiver. Le standard définit également le processus d'élimination (édition d'un bordereau d'élimination numérique à faire viser par l'administration des archives. https://www.ateliers.modernisation. gouv.fr/ministeres/projets_adele/a103_archivage_ elect/public/standard_d_echange_d/folder_contents).