COLLECTION
LES GUIDES DE LA CONFIANCE DE LA FNTC

Fédération des
Tiers de Confiance

GUIDE
POUR LA CONFIDENTIALITÉ DES ARCHIVES NUMÉRIQUES

www.fntc.org

Par le groupe de travail « archivage électronique et coffre-fort électronique » de la Fédération des Tiers de Confiance

DANS LA COLLECTION LES GUIDES DE LA CONFIANCE DE LA FNTC :

téléchargement : www.fntc.org/publications/les-guides/les-guides-de-la-confiance/

Guide pour la confidentialité des archives numériques (juin 2015)

Vade-mecum juridique de la dématérialisation des documents, 7ème édition (juin 2015)

Guide de la cession électronique de créances (mars 2014)

Guide de l'interopérabilité des coffres-forts électroniques (mars 2014)

Guide de la signature électronique (octobre 2013)

Guide de la traçabilité (octobre 2013)

Guide Normes et Labels de la dématérialisation (octobre 2013)

Le bulletin de paie électronique (mars 2012)

Du livret ouvrier au bulletin de paie électronique (mars 2012)

Guide du Document Hybride et de la Certification 2D (nov. 2011)

Fascicule e-paie « le rôle du bulletin de paie dans la reconstitution de carrière » (mars 2011)

Guide du vote électronique, nouvelle édition (mars 2011)

Guide de l'archivage électronique et du coffre-fort électronique (nov. 2010)

Au-delà de la migration Etebac (sept. 2010)

Guide de la Facture électronique (janv. 2010)

Du mandat au mandat électronique (déc. 2009)

PROCHAINE PARUTION

Guide de mise en œuvre du Relevé d'Identité du Coffre-fort numérique

SOMMAIRE

2 - INTRODUCTION

Les affaires Prism et Snowden, les risques accrus faces à la « guerre froide » numérique entre États ainsi que les nuisances des organisations criminelles sont bien réelles. Les organisations gouvernementales veillent à protéger les actifs informationnels et les systèmes d'informations français, notamment par rapport à l'étranger. Elles défendent les droits des citoyens sur leurs données personnelles et médicales. L'objet d'attention de ces organisations est notamment la « donnée » au sens « information dans un système d'informations ». Il s'agit donc d'un domaine d'experts essentiellement composé d'informaticiens, de systèmes et de réseaux.

Les archives numériques sont, à ce titre, des données informatiques. Nous sommes donc dans le même objet d'attention. A une différence près : il s'agit du domaine de l'archiviste !

Le besoin fonctionnel de l'archiviste est différent du besoin du responsable SSI[1]. En effet, l'archiviste a vocation à conserver et à communiquer alors que les rôles du SSI ont tendance à limiter la communication d'informations. Leurs intérêts semblent opposés ; pourtant ils peuvent se compléter. L'archiviste est particulièrement sensible à la confidentialité, alors que le responsable de la sécurité possède l'intégrité dans ses gênes.

Il semble néanmoins nécessaire d'établir un langage commun. ***Informat***ique, ***Informat***ion, donnée, archives. L'objectif ne semble pas si éloigné : informer. S'il n'y a pas d'information, il n'y a pas d'informaticiens ni d'archivistes. Il convient de rétablir le dialogue pour faire en sorte que l'archiviste n'expose pas ses archives à un risque de divulgation et ne sacrifie pas l'intérêt fondamental des archives – la consultation – au besoin de confidentialité.

Les archives numériques existent pour être consultées, certaines servent également de preuves et d'autres constituent un patrimoine historique ou scientifique. Le besoin d'intégrité de ces archives, leur accessibilité et leur pérennité ont été les motivations premières pour développer les solutions d'archivage électronique qui contribuent à la modernisation de notre société.

Notre époque actuelle est de plus en plus marquée par la problématique de la confidentialité des informations numériques au sens large. La protection des données face aux menaces de l'internationalisation des opérateurs, du hacking, voire des exploitants internes eux-mêmes devient donc une préoccupation majeure.

Comment concilier les besoins d'accessibilité aux exigences de confidentialité dans un contexte d'archivage numérique ? Le groupe de travail Archivage de la Fédération des Tiers de Confiance (FNTC) publie ce Guide sur ce sujet en abordant notamment l'impact des solutions de chiffrement sur la pérennité et l'intégrité des archives numériques.

Ce Guide d'usage pédagogique posera les principes structurants pour la gestion de la confidentialité des archives numériques. Sans préconiser des solutions particulières, il permettra d'identifier les risques et de choisir les défenses les plus adaptées pour y répondre.

1 .SSI : Sécurité des Systèmes d'Information

3 - NOTE DE SYNTHÈSE

Le groupe de travail Archivage de la FNTC a choisi de partir du besoin de confidentialité d'un point de vue utilisateur, puis réglementaire, pour, ensuite, développer le panorama des solutions permettant de répondre à ce besoin.

Ce Guide reprendra le besoin des différents acteurs impliqués dans la confidentialité des données au sens large et des archives numériques en particulier. Ces acteurs sont l'archiviste, le Responsable de la Sécurité des Systèmes d'Information (RSSI), le Correspondant Informatique et Liberté (CIL) ou le Records Manager qui peuvent avoir une approche différente du sujet.

Le besoin oppose en apparence la confidentialité et l'accessibilité. Ce besoin se positionne différemment dans le temps (il augmente ou diminue dans le temps) et dans l'espace, selon le niveau d'exposition des archives numériques et leur sensibilité.

---------- Réglementation ----------

La dimension réglementaire et juridique du chiffrement doit être également étudiée, notamment les réglementations internationales et européennes, les procédures d'enquêtes, la localisation, le régime des formalités, et les contraintes propres à certains secteurs (bancaire, santé, archives publiques). Les réglementations relatives à la protection des données à caractère personnel et celles relatives aux questions de sécurité publiques peuvent être difficiles à concilier.

---------- Défense en profondeur ----------

L'approche de base pour la confidentialité des archives numériques, déclinée du principe de défense en profondeur, nécessite d'être développée dans un contexte d'archivage numérique : Analyser les risques, construire un « bastion de conservation », cloisonner les fonds, étanchéifier les moteurs de recherche, et surtout, sécuriser les accès seront développés en tant que principes essentiels. Il semble opportun de formaliser la façon dont il convient de concevoir un système d'archivage électronique, tant d'un point de vue de l'infrastructure à mettre en œuvre que des fonctionnalités de sécurité attendues.

---------- Option de chiffrement ----------

Le chiffrement des archives est une barrière supplémentaire envisageable dans un système de défense en profondeur. Il s'agit de solutions de « confidentialité renforcée », mais en aucun cas d'une alternative permettant de sécuriser un fonds d'archives dans un environnement de conservation non maîtrisé.

Pour l'archivage numérique, il convient d'identifier deux périmètres d'application potentiels du chiffrement : le document d'archive lui-même et les métadonnées associées. Les métadonnées sont généralement sous plusieurs supports : en base, dans les fichiers associés au fichier d'archive, dans les index des instruments et moteurs de recherches, etc. La donnée à protéger est donc potentiellement dans plusieurs endroits différents pour lesquels il existe différentes approches pour la confidentialité.

L'exposition des archives n'est pas la même lors des échanges et pendant la conservation. L'échange (pour le versement, la consultation et la réversibilité), lorsqu'il transite via des réseaux partagés, nécessitera plus de moyens pour la confidentialité que pendant la conservation, notamment si les espaces de conservation ne sont pas exposés.

Un chiffrement des archives pendant la conservation peut procurer une protection supplémentaire, notamment face aux risques internes. La solution de chiffrement dépendra de deux paramètres principaux :

- où se positionne le chiffrement ? Selon la position des mécanismes de chiffrement et de déchiffrement dans les différentes « couches » matérielles et applicatives d'un Système d'Archivage Électronique (SAE), le niveau de protection sera différent ;
- qui doit détenir les clés de chiffrement/déchiffrement ? La solution de chiffrement varie si la détention des clés est réalisée par l'utilisateur, ou par l'un des composants (physiques ou applicatifs) ou encore par un tiers de confiance.

Le principe retenu est que plus le secret est détenu par les couches hautes du système, voire par l'utilisateur lui-même, plus la confidentialité est renforcée et plus le système est complexe à mettre en œuvre et à exploiter.
Évoquer le chiffrement des archives tant que le périmètre d'application n'est pas clairement défini ne garantit en rien un niveau élevé de confidentialité. A l'heure où certain opérateurs annoncent qu'ils chiffrent mais sans préciser quoi ni comment, il est important de clarifier les usages des opérateurs pour renforcer la confiance des utilisateurs et du marché.

---------- Impact du chiffrement ----------

L'implémentation de technologies de chiffrement, pour une solution d'archivage numérique en particulier, induit un ensemble de considérations archivistiques à prendre en compte pour la gestion de l'intégrité des archives, de leur accessibilité et de leur pérennité.
Des questions de fond se posent dans ce contexte et notamment :

- les empreintes pour l'intégrité doivent-elles être calculées avant ou après le chiffrement ?
- comment indexer des documents chiffrés ?
- comment traiter la confidentialité des métadonnées ?
- comment traiter la problématique de transchiffrement en cas d'obsolescence des formats de chiffrement ?
- quel impact sur les capacités des systèmes en termes de performance ?
- doit-on chiffrer les systèmes de secours et les sauvegardes ?
- …

Les réponses sont attendues par les organismes publics ou privés qui étudient une solution de sécurité renforcée.

------- Le Positionnement du service d'archivage ------

Le choix du positionnement du service d'archivage est important dans la stratégie de confidentialité. Il s'agit de choisir le niveau d'exposition au risque par rapport à l'extérieur et à l'intérieur. Ce niveau ne sera pas le même pour une solution interne, ou une externalisation chez un tiers archiveur ou encore un stockage dans le Cloud. Chaque modèle présente des avantages, des risques et des coûts différents.

4 - LA RÉALITÉ DES BESOINS DE CONFIDENTIALITÉ

Les besoins de confidentialité des archives sont variables : ils évoluent dans le temps et dans l'espace, selon les niveaux d'exposition aux risques et selon la sensibilité même de l'information qu'elles contiennent.

4.1 - Le temps

De façon générale, les archives sont caractérisées par une dimension temporelle lente, bien différente des NTIC[2]. Pour prévenir la vélocité, et par conséquent, l'obsolescence des technologies et des formats de conservation, les systèmes d'archivage numérique utilisent de préférence des formats normalisés ou standardisés, et effectuent des migrations, si nécessaire, afin de préserver la pérennité des archives.

Le niveau de confidentialité peut se réduire ou augmenter dans le temps selon le type d'archive : un rapport financier peut être hautement confidentiel avant d'être publié, un document classifié Confidentiel Défense pourra être déclassifié. Inversement, l'accès à une archive pourra être restreint, voire interdit, en vertu du droit à l'oubli… **Inversement, le droit à l'oubli force à restreindre, voire à interdire tout accès à une archive.**

Parfois, la relation au temps est une différence quasi culturelle selon les organismes, notamment sur la question des données personnelles : pour les archivistes, plus c'est ancien, moins c'est confidentiel car les archives présentent un intérêt de recherche pour les historiens ou les généalogistes alors que c'est l'inverse pour les organismes français ou européens Chargés de la protection des données qui demandent d'appliquer le droit à l'oubli. Ceci peut amener des débats animés où sont opposés les enjeux historiques et les droits des citoyens.

4.2 - L'espace

Historiquement, les archives étaient confortablement conservées dans des salles protégées et accessibles aux seuls archivistes. Le numérique change la donne : lorsque le besoin induit d'exposer les archives aux risques liés à la « virtualisation » des espaces de conservation, dans le Cloud notamment, ou si les fonds sont accessibles via le Web, les moyens et méthodes pour assurer la confidentialité seront importants. A l'opposé, un système interne très protégé et peu exposé sur l'extérieur nécessitera moins de moyens additionnels pour préserver la confidentialité.

4.3 - La sensibilité du contenu

A chaque contenu sa sensibilité et les niveaux de confidentialité associés. Le niveau de sensibilité d'un document déterminera la classification et, donc, le besoin de confidentialité ainsi que les différentes solutions permettant d'y répondre. La solution unique n'existe malheureusement pas.
Les archives nécessitent d'être communiquées, mais de manière maîtrisées. Le besoin de partage est souvent oublié et peut rendre inadaptées des solutions de confidentialité performantes, car vues comme trop contraignantes. Les archives risquent fort alors d'être tout de même partagées, mais en dehors de tout système sécurisé.

2. Nouvelles Technologies de l'Information et de la Communication : outils informatiques utilisés dans le traitement et l'échange d'informations.

5 - ASPECTS JURIDIQUES DE LA CONFIDENTIALITÉ

Il apparaît clairement que le besoin de confidentialité est variable. Il est largement précisé dans le droit sur un périmètre sectoriel, national ou international.
Les aspects juridiques de la confidentialité sont développés dans ce chapitre autour de trois thématiques :

- la confidentialité des données archivées et le droit ;
- le cadre juridique pour les outils techniques permettant d'assurer la confidentialité des données ;
- l'approche internationale de la confidentialité pour l'archivage des données.

5.1 - La confidentialité des données archivées et le droit

Peu de textes traitent expressément de la confidentialité des données et encore moins de leur archivage. La confidentialité est identifiée par la norme ISO 27001 comme un élément constitutif de la sécurité à côté de la disponibilité et de l'intégrité. La confidentialité est identifiée par la norme ISO 27001 comme un critère de sécurité au même titre que la disponibilité et l'intégrité. Or, cette sécurité doit être assurée depuis l'émission de la donnée jusqu'au terme de l'archivage.

La confidentialité des données est un impératif présent pendant tout le cycle de leur exploitation en ce incluse la période d'archivage.

Ceci étant, les garanties à prendre diffèrent selon la qualité des données concernées et, au vu de la pluralité de textes applicables et des situations concernées (finalités/objectifs impartis à un traitement de données), seules deux catégories de données seront ici abordées.

En effet, il est possible de distinguer :

- **les données confidentielles « par nature »**, données qui, en tout état de cause, sont soumises à une obligation de confidentialité imposée par le Code pénal[3] par la Loi « Informatique et Libertés »[4](5.1).;
- **les données à caractère personnel** dont l'archivage, en tant que traitement au sens de la loi « Informatique et Libertés », est soumis à des exigences de confidentialité (5.1.2).

---

3. Sont concrètement concernées les « informations à caractère secret » expressément visées par l'article 226-13 du Code pénal (secret professionnel) : « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. »

4. Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. Spécifiquement, les articles 8, 9, 25 et 26 font apparaître que les données dites « sensibles », donc confidentielles par nature :
- les origines raciales ou ethniques (art. 8) ;
- les opinions politiques, philosophiques ou religieuses (art. 8) ;
- l'appartenance syndicale des personnes (art. 8) ;
- les données qui sont relatives à la santé (art. 8) ;
- les données relatives à la vie sexuelle des personnes (art. 8) ;
- les données relatives aux infractions, condamnations et mesures de sûreté relatives aux personnes (art. 9) ;
- les données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (art. 25) ;
- les données qui par leur nature, leur portée ou leurs finalités, excluent des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou régle mentaire (art. 25) ;
- les appréciations sur les difficultés sociales des personnes (art. 25) ;
- les données biométriques nécessaires au contrôle de l'identité des personnes (art. 25) ;
- les données relatives à la sûreté de l'Etat, la défense ou la sécurité publique (art. 26).

5.1.1 - Archivage des données confidentielles "par nature"

Nombre de données sont confidentielles par nature du fait de leur sensibilité. Tel est le cas, par exemple, des données de santé (5.1.1.1) et des données bancaires (5.1.1.2). Cela étant, cette catégorie spécifique n'est pas figée et reste susceptible d'intégrer de nouvelles données, telles celles soumises à la protection du secret des affaires.

5.1.1.1 - La confidentialité de l'archivage des données de santé

La confidentialité des données de santé est une exigence intrinsèquement liée à leur nature. Cette obligation relève de diverses dispositions prescrites au titre du secret professionnel (article 226-13 du code pénal[5]), reprises par le code de la santé publique (article L.1110-4 et L.1111-7 du CSP) et par la Loi « Informatique et Libertés » et son décret d'application[6].

Il convient de noter qu'en l'état actuel du droit positif[7], même si la notion de données de santé n'est pas légalement définie, elle reçoit toutefois une acception très large, faisant aussi bien référence à l'état de santé d'une personne qu'aux facteurs pouvant l'expliquer ou aux prestations de services de santé (prévention, diagnostic ou soins). Précision d'importance car, au titre de la réglementation applicable à la protection des données personnelles (quel que soit le texte de référence), la collecte et le traitement des données relatives à la santé (les données de santé étant des données à caractère personnel au sens de la loi « Informatique et Libertés ») sont par principe interdits. De fait, les autorisations sont très strictement encadrées par la loi « Informatique et Libertés » et visent exclusivement *« **les traitements nécessaires aux fins de la médecine préventive**, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé **et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel** prévue par l'article 226-13 du Code pénal »*. Afin d'encadrer l'hébergement des données de santé à caractère personnel, la loi n°2002-303[8] a notamment introduit au sein du Code de la santé publique (CSP) l'article L.1111-8 permettant aux professionnels de santé, aux établissements de santé et aux personnes concernées de déposer les données de santé recueillies *« auprès de personnes physiques ou morales agréées à cet effet »*. De plus, les articles R.1111-9 et suivants du CSP, codifiés par le décret n°2006-6 du 4 janvier 2006[9], encadrent le dispositif d'agrément de l'hébergeur de données de santé sur support informatique.

L'obligation de secret professionnel *« **s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé**.[…] »* (article L.1110-4 du CSP). Ainsi, au vu de l'article R.1111-9 du CSP, les hébergeurs de données sont tenus de définir et de mettre en œuvre *[…] **une politique de confidentialité et de sécurité**, destinée notamment à **assurer le respect des exigences de confidentialité et de secret** prévues par*

5 . Voir note de bas de page 3 en page 10.

6 . Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

7 . La proposition de Règlement européen sur la protection des données offre une définition (la seule) des «données concernant la santé» comme étant « toutes données à caractère personnel relatives à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne ».

8 . Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JORF du 5 mars 2002 p.4118 texte n°1.

9 . Décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires), JORF n°4 du 5 janvier 2006 page 174, texte n°14.

les articles L.1110-4 et L.1111-7, ***la protection contre les accès non autorisés ainsi que la pérennité des données*** *[…] ».*

A noter que le récent Projet de loi relatif à la santé[10] propose notamment d'étendre ce secret professionnel aux personnels des services sociaux et médico-sociaux, et d'imposer à tous les acteurs de la chaîne le respect des référentiels de sécurité et d'interopérabilité mis en œuvre par le groupement d'intérêt public chargé du développement des systèmes d'information de santé. De plus, ce projet tend à organiser la mise en œuvre du nouveau « Système national des données de santé ». Enfin, il contient également des dispositions permettant au gouvernement de prendre, par ordonnance, des mesures d'amélioration et de simplification du système de santé et notamment des mesures aux fins d'harmonisation selon les dispositions de l'article L.1111-8 du code de la santé publique relatives aux procédures d'agrément des hébergeurs de données de santé.

5.1.1.2 - La confidentialité de l'archivage des données bancaires

A l'image des données de santé, le régime des données bancaires se retrouve également à la jonction entre le régime des données à caractère personnel, le secret professionnel et les obligations imposées aux établissements bancaires et financiers (prévention contre le blanchiment de capitaux).

Le secret bancaire[11] comprend à la fois l'obligation de discrétion, sanctionnée civilement, et l'obligation de respecter le secret professionnel sanctionnée par l'article 226-13 du Code pénal, **pour les entreprises**, notamment d'une amende maximale de 75.000 € et d'une éventuelle interdiction d'exercice de la profession.

Les banques étant assujetties à une obligation particulière de vigilance à l'égard de la clientèle, elles ont pour obligation de recueillir un certain nombre d'informations. Ainsi, aux termes de l'article L.561-6 du Code monétaire et financier (CMF) *« Avant d'entrer en relation d'affaires avec un client, les personnes mentionnées à l'article L.561-2* ***recueillent les informations relatives à l'objet et à la nature de cette relation et tout autre élément d'information pertinent sur ce client.[…]*** *»*, l'article L.561-12 du CMF[12] fixant la durée de conservation de ses informations.

Or, si de très nombreuses informations sont recueillies et traitées par les établissements bancaires, ceux-ci sont également soumis à cette obligation de **secret professionnel**. En effet, l'article L.511-33 impose par principe que *« **Tout membre** d'un conseil d'administration*

---

10 . Projet de loi relatif à la santé, n°2302, déposé le 15 octobre 2014, disponible sous le lien : http://www.legifrance.gouv.fr/affichLoiPreparation.do?idDocument=JORFDOLE000029589477&type=contenu&id=2&typeLoi=proj&legislature=14

11 . Voir pour de plus amples détails, Ouvrage collectif du Cabinet Caprioli & Associés, La Banque en Ligne et le Droit, RB édition, Les essentiels de la banque et de la finance, 2014.

12 . Article L.561-12 du Code monétaire et financier : « Sous réserve de dispositions plus contraignantes, les personnes mentionnées à l'article L.561-2 conservent pendant cinq ans à compter de la clôture de leurs comptes ou de la cessation de leurs relations avec eux les documents relatifs à l'identité de leurs clients habituels ou occasionnels. Elles conservent également, dans la limite de leurs attributions, pendant cinq ans à compter de leur exécution, les documents relatifs aux opérations faites par ceux-ci, ainsi que les documents consignant les caractéristiques des opérations mentionnées au II de l'article L.561-10-2.
Les personnes mentionnées au 9° de l'article L.561-2 satisfont à cette obligation en appliquant les mesures prévues à l'article L.561-13. ».

et, selon le cas, d'un conseil de surveillance et toute personne qui, à un titre ***quelconque, participe à la direction ou à la gestion d'un établissement de crédit ou d'un organisme*** *mentionné au 5 de l'article L.511-6 ou qui est* ***employée par l'un de ceux-ci est tenu au secret professionnel****. ».* Cela étant, la suite de l'article et l'article L.511-34 du CMF mettent en valeur les exceptions à ce principe. Tel est le cas, par exemple, des échanges d'informations au sein d'un même groupe afin de permettre une prévention accrue du risque de blanchiment de capitaux et de financement du terrorisme.

Il est donc essentiel pour un établissement bancaire et financier ou un prestataire travaillant avec ces derniers (car certaines exigences en la matière leur sont à ce titre imposées) de veiller à sécuriser l'archivage de telles données, en se référant notamment, mais pas exclusivement, à l'Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque[13] qui se substitue au Règlement n°97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement[14].

Focus : sanction CNIL

En pratique, la CNIL a eu l'occasion de prononcer un avertissement envers la filiale d'une banque par une délibération du 21 juin 2012[15] du fait du partage du système d'information entre plusieurs entités au sein du groupe bancaire, et de le rendre public sur son site internet.

L'accès à des données bancaires confidentielles, protégées par le secret bancaire, ayant été rendu possible aux salariés de cette dernière structure, la CNIL condamne ce manque d'étanchéité pris « sans égard pour la conformité bancaire ».

La CNIL a ouvert une concertation avec les professions bancaires et financières le 6 octobre 2014[16] sur un futur pack de conformité CNIL « Banques » afin de faire un état des lieux complet des besoins et des pratiques. Le pack « Banques » de la CNIL a pour objectif de réviser et d'adapter les procédures existantes, mais aussi de traiter de questions liées à la lutte contre les fraudes.

511.3 - Bientôt la confidentialité de l'archivage des données couvertes par la protection du secret des affaires

La sphère des données confidentielles « par nature » pourrait bientôt prendre une ampleur inédite en recouvrant les données issues du secret des affaires. En effet, le 16 juillet 2014 a été

13 . *Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution, JO du 5 novembre 2014.*

14 . *Disponible à l'adresse : http://www.acp.banque-france.fr/fileadmin/user_upload/acp/Controle_prudentiel/ reglt97-02-consolide.pdf.*

15 . *Disponible sous le lien : http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2012-176_EURO_INFORMATION.pdf*

16 . *Actualité CNIL « Les packs de conformité : un succès grandissant » disponible sous le lien : http://www.cnil.fr/les-themes/argent/article/article/les-packs-de-conformite-un-succes-grandissant/*

présentée une proposition de loi relative à la protection du secret des affaires[17]. S'inscrivant dans une démarche européenne plus large, caractérisée par la proposition de directives sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites[18], cette proposition de loi entend instituer la protection de toute information : i) qui ne présente pas un caractère public, ii) qui s'analyse comme un élément à part entière du potentiel de son détenteur et revêt en conséquence une valeur économique, iii) qui fait l'objet de mesures de protection raisonnables pour en conserver le caractère non public.

Toute atteinte au secret des affaires ainsi défini engagerait non seulement la responsabilité civile de son auteur, mais également sa responsabilité pénale, le fait de révéler sans autorisation de telles données étant puni de 3 ans d'emprisonnement et de 375 000 euros d'amende.

Il deviendra donc essentiel, pour les personnes dépositaires de secrets des affaires, de prendre des mesures de protection « équilibrées », aptes non seulement à valider la protection (la mesure de protection raisonnable étant l'un des critères) mais également à s'opposer à toute mise en jeu de sa responsabilité, notamment lors de l'entrée en possession des données de ses partenaires.

5.1.2 - La confidentialité des données à caractère personnel du fait de leur traitement

Au-delà du traitement de données confidentielles « par nature », tout traitement de données à caractère personnel est soumis à un certain nombre d'obligations. Or, l'archivage est un traitement en lui-même. A ce titre, tout archivage de données à caractère personnel est soumis à ces obligations.

Si la Directive 95/46/CE[19] fait explicitement référence à la confidentialité des traitements, et non des données, la notion sert exclusivement à encadrer l'activité des sous-traitants. En revanche, aucune référence explicite à la confidentialité n'est présente dans la proposition de Règlement européen[20] destinée à remplacer cette Directive, ni dans la loi n°78-17[21] dite loi

17 . *Proposition de loi de MM. Bruno LE ROUX et Jean-Jacques URVOAS et plusieurs de ses collègues relative à la protection du secret des affaires, n°2139, déposée le 16 juillet 2014, disponible sous le lien : http://www.assemblee-nationale.fr/14/dossiers/protection_secret_affaires.asp.*

18 . *PE et Cons. UE, prop. dir. COM(2013) 813 final, 28 nov. 2013, sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, disponible sous le lien : http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/131128_proposal_fr.pdf.*

19. *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Disponible sous le lien : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML.*

20. *La proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)- Résolution du Parlement européen du 12 mars 2014. Disponible sous le lien : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR.*

21. *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (JORF du 7 janvier 1978 page 227) modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (JORF n°182 du 7 août 2004 page 14063 texte n°2).*

« Informatique et libertés ». De fait, l'article 34 de la loi impose au responsable de traitement *« de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées,* ***ou que des tiers non autorisés y aient accès****. […] »* sous peine de sanctions administratives (sanctions CNIL) et/ou pénales (peines de 5 ans d'emprisonnement et de 300.000 euros prévues par l'article 226-17 du Code pénal). La confidentialité est ici intrinsèquement liée à l'accès aux données, c'est une garantie nécessaire et conjointe de la sécurité que doit apporter le responsable de traitement, mais également tout sous-traitant sous ses instructions (article 35).

La Recommandation n°2005-213[22] de la CNIL vient aiguiller les entreprises et organismes du secteur privé dans la gestion de l'archivage des données à caractère personnel. Quel que soit le niveau d'archives concerné (archives courantes, intermédiaires et définitives), pour la sécurité des données, la Recommandation préconise de mettre en œuvre une séparation logique des données archivées (avec gestion des habilitations), des dispositifs sécurisés lors de tout changement de support de stockage des données archivées, des dispositifs de traçabilité des consultations des données archivées…

5.2 - Les outils techniques permettant d'assurer la confidentialité des données

Le chiffrement, outil de la cryptologie, s'entend de tout processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible[23]. La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[24] (LCEN) définit, quant à elle, les « moyens de cryptologie » comme étant *« tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement* ***pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.***[25]*»* .

Si, jusqu'en 1990, les moyens de cryptologie étaient soumis à un régime restrictif, celui-ci s'est progressivement libéralisé. Depuis l'adoption de la LCEN, où le principe de liberté d'utilisation des moyens de cryptologie a été consacré par son article 30, les règles pour la fourniture, le transfert, l'importation et l'exportation des moyens de cryptologie ont été assouplies. Seuls la fourniture et le transfert d'un moyen de cryptologie ***n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité*** (donc assurant la confidentialité) restent soumis à une déclaration préalable auprès du premier ministre en cas d'importation (hors UE) et à autorisation du premier ministre en cas d'exportation.

---

22. Délibération n°2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel, JORF n°272 du 23 novembre 2005 page, texte n°81.

23. V. Eric A. Caprioli, Le nouveau régime juridique de la cryptologie (suite aux deux décrets du 24 février 1998), Supplément au bulletin d'actualité du Lamy Droit de l'informatique, n°101, mars 1998, p. 1 et s.

24. JORF n°0143 du 22 juin 2004 page 11168, texte n°2

25. Article 29 de la LCEN.

Focus : CNIL- ANSSI : même combat

Les risques informatiques importants sont maîtrisables si on prend les bonnes mesures. La CNIL s'appuie de plus en plus fréquemment sur les Recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) en matière de sécurité informatique.

Le chiffrement des données constitue une précaution reconnue pour bon nombre de traitements (ex : envoi de courriers électroniques, données stockées sur une tablette…). Dans le cadre des services de coffres-forts numériques destinés aux particuliers, la CNIL préconise que « les données [soient] chiffrées avec une clef, maîtrisée uniquement par l'utilisateur, conforme aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques éditées par l'ANSSI dans son référentiel général de sécurité[26] à l'annexe B1 » (point 3 de la délibération n°2013-270 du 19 septembre 2013).

Considérée comme une précaution majeure, le chiffrement des données devient de plus en plus une obligation, y compris au niveau communautaire (Cf. Règlement (UE) n°611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques – JOUE du 26 juin 2013, L.173, p.2 et s[27]) au même titre que d'autres mesures technologiques que les prestataires devront prendre en compte.

Cela étant, l'article 39 de la LCEN précise que ces dispositions n'affectent pas le régime dérogatoire antérieur à destination des moyens de cryptologie en matière d'arme et de défense nationale.

Le tiers archiveur peut être considéré comme fournissant des prestations de cryptologie entendu au sens de l'article 29 al. 2 de la LCEN comme : *« toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie »*.

La fourniture de prestation de cryptologie doit être, quant à elle, déclarée auprès du premier ministre. Le décret n°2007-663 du 2 mai 2007 pris en application des articles 30, 31 et 36 de la LCEN et relatifs aux moyens et aux prestations de cryptologie[28] et l'arrêté du 29 janvier 2015 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et prestations de cryptologie[29] sont venus préciser les

26. Référentiel Général de sécurité : https://references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf

27. L'article 4 dispose : « 2. Les données sont considérées comme incompréhensibles si :
a) elles ont été cryptées en mode sécurisé à l'aide d'un algorithme normalisé et la clé utilisée pour les décrypter n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser ; ou
b) elles ont été remplacées par leur valeur hachée, calculée à l'aide d'une fonction de hachage normalisée à clé cryptographique, et la clé utilisée pour les hacher n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser ».

28. J.O. du 4 mai 2007, p.7865 et s. V. Eric A. Caprioli, La nouvelle réglementation sur la cryptologie : un cadre juridique enfin complet, Comm. Com. Electr. Octobre 2007, comm.128. .

29. J.O. du 19 février 2015 p. 3081 et s.

formalités applicables en matière de cryptologie. En effet, si le décret n°2007-663 est venu décrire les différentes formalités applicables (dispense de formalité préalable, déclaration et autorisation), il détaille également des objets ou équipements auxquels ces formalités sont applicables, l'arrêté du 29 janvier 2015 apportant, quant à lui les formulaires nécessaires à la réalisation de ces formalités.

La LCEN a entouré ses principes **d'une sanction administrative (interdiction de mise en circulation du moyen de cryptologie concerné) et de sanctions pénales**. Par exemple, le fait de ne pas satisfaire à l'obligation de déclaration sera puni d'un an d'emprisonnement et de 15 000 Euros d'amende quand le fait d'exporter un moyen de cryptologie sans autorisation encourra deux ans d'emprisonnement et 30 000 Euros d'amende.

A noter que, longtemps commandés par les nécessités de la défense nationale et de la sécurité de l'État, les moyens de cryptologies sont à l'heure actuelle entendus comme étant un sous-ensemble parmi les marchandises et technologies dites *« à double usage »* (civil et militaire) dont l'arrangement de Wassenaar[30] et le Règlement (CE) n°428/2009[31] dictent les lignes directrices en matière d'exportation. En effet, ce dernier définit les biens à double usage comme étant *« les produits, y compris les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire ; ils incluent tous les biens qui peuvent à la fois être utilisés à des fins non explosives et entrer de manière quelconque dans la fabrication d'armes nucléaires ou d'autres dispositifs nucléaires explosifs »*. A noter que ce règlement a été récemment modifié par le règlement n°599/2014[32] déléguant, au profit de la Commission, le pouvoir d'adopter des actes en vue de retirer des destinations du champ d'application des autorisations générales d'exportation de l'Union européenne si ces destinations sont frappées d'un embargo sur les armes.

Focus : la responsabilité des personnes fournissant des prestations de cryptologie.

L'article 32 de la LCEN établit que *« Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions. »*

Cet article institue ainsi une responsabilité de plein droit à la charge des personnes fournissant des prestations de cryptologie à des fins de confidentialité. Inversant la

30. *Arrangement de Wassenaar relatif au contrôle multilatéral des exportations pour les armes conventionnelles et les marchandises et technologies à double usage : Voir http://www.wassenaar.org*

31. *Règlement (CE) N° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage, JOCE L.134 du 29 mai 2009, p.1 et s, disponible à l'adresse : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:fr:PDF*

32. *Règlement (UE) n°599/2014 du parlement européen et du conseil du 16 avril 2014 portant modification du règlement (CE) n°428/2009 du Conseil instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage, JOCE L.173 du 12 juin 2014, p.79 et s, disponible à l'adresse : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:JOL_2014_173_R_0004&from=FR*

charge de la preuve, cette disposition oblige ces personnes à démontrer qu'elles n'ont commis aucune faute intentionnelle ou de négligence pour s'opposer à la mise en œuvre de leur responsabilité en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données ayant entraîné un préjudice.

Dès lors, toute conservation des conventions secrètes effectuée par un prestataire au profit d'un de ses clients pourrait tomber sous l'emprise de ce texte. Une analyse des risques concernant cette pratique est donc nécessaire.

5.3 - Approche internationale de la confidentialité de l'archivage des données

Dans une économie mondialisée, la confidentialité des données est plus que jamais requise. A l'heure où le fait de détenir l'information peut constituer un avantage décisif, les pratiques d'espionnage se multiplient. Mais il n'y a pas que l'espionnage qui peut mettre à mal la confidentialité d'une donnée.

Ainsi, si les États-Unis ont défrayé la chronique avec des textes emblématiques tels que le *Patriot Act*, d'autres pays se dotent de dispositions similaires, c'est-à-dire aussi intrusives.

Concrètement, le *Patriot Act*[33] a institué, par le biais de sa section 21, une pratique nourrie de collecte de données et d'interception de communications. En effet, cet article autorise le Gouvernement, sans qu'il soit besoin de solliciter un mandat, à saisir *« toute chose tangible »* pouvant avoir un rapport avec une enquête antiterroriste, et ce, même si la personne concernée n'est pas, en elle-même, soupçonnée de terrorisme. Cette collecte a été étendue à tout renseignement étranger par la Section 702 du *Foreign Intelligence Surveillance Act*.

Une entreprise recourant aux services de prestataires américains en matière d'archivage/de stockage devra prendre garde quant à la confidentialité toute relative de ses données ainsi conservées.

Focus : Microsoft tenue de communiquer aux autorités américaines les données de ses clients stockées à l'étranger

Le 25 avril 2014, la Cour fédérale du district de New York s'est prononcée sur la demande de Microsoft tendant à faire annuler partiellement un mandat de recherche et de saisie, délivré sur le fondement du « stored communication act » (SCA), qui exigeait qu'elle produise le contenu des emails de clients stockés sur un serveur à Dublin (Irlande).

Microsoft estimait que la référence du SCA à l'article 41 du code de procédure pénale (qui comporte une limitation de l'étendue territoriale du mandat) écartait la compétence des juridictions américaines pour délivrer un mandat de saisie et de recherche de données situées hors du territoire américain.

33. Certaines inflexions de ce texte sont en cours comme l'USA Freedom Act, https://beta.congress.gov/bill/113th-congress/house-bill/3361, (à l'état de projet de loi).

Le juge a tout d'abord précisé que le 4ème amendement (qui protège contre les perquisitions abusives aux domiciles des particuliers) ne trouvait pas à s'appliquer dans le cadre de perquisitions et de saisies de données, car les serveurs ne constituent pas des domiciles virtuels à l'instar des domiciles « physiques ». Il a alors expliqué que le SCA avait été notamment adopté afin d'offrir une protection constitutionnelle particulière aux recherches et saisies de données. Ce faisant, le juge a démontré que le mandat prévu par le SCA n'était pas un mandat traditionnel.

Dès lors, le juge a considéré qu'ayant son siège aux États-Unis et en sa possession les informations recherchées, Microsoft se devait de les lui communiquer, quand bien même les données seraient stockées en dehors du territoire américain. Ce faisant, le juge n'a pu que rejeter la demande de Microsoft tendant à l'annulation partielle du mandat de recherche.

Cette décision rend donc la communication des données d'un prestataire *Cloud* américain totalement indépendante de leur lieu de stockage. Seul le critère du lieu d'établissement de la société semble dorénavant pris en compte. Cette décision va donc appeler à la prudence et à la réflexion des clients des prestataires *Cloud* américains, notamment en cas de stockage de données d'une certaine sensibilité.

Cela étant, d'autres pays disposent de textes octroyant à leurs forces de l'ordre la possibilité d'organiser une recherche approfondie au sein de systèmes informatiques, et *a fortiori,* au sein d'archives numériques.

Tel est le cas au Canada, où **l'article 83.28 du Code criminel** spécifie qu'un agent de la paix peut, pour la conduite d'une enquête relative à une infraction de terrorisme, et s'il a obtenu le consentement préalable du procureur général, demander à un juge une ordonnance autorisant la recherche de renseignements. Tel est également le cas du *Terrorism Act* mis en œuvre par le Royaume-Uni depuis l'année 2000, dont l'article 42 permet d'effectuer des perquisitions dans des maisons après avoir reçu un mandat d'un juge, fondé sur des *« doutes raisonnables »*.

En France, la loi relative à la programmation militaire pour les années 2014 à 2019 (LPM)[34], est venue doter l'État français des mêmes moyens d'action que ses homologues étrangers en matière de « cyberdéfense » et « cybersécurité ». En effet, si la loi LOPPSI 2[35] octroyait la possibilité, sur autorisation du juge d'instruction, de mettre en place un dispositif technique ayant pour objet d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre (articles 706-102-1 à 706-102-9 au Code de la procédure pénale), la LPM permet désormais un accès « administratif » aux données de connexion, c'est-à-dire sans la nécessité de solliciter l'autorisation d'un juge[36].

En pratique, le nouvel article L.246-1 du code de la sécurité intérieure permettra le recueil, notamment auprès des opérateurs de communications électroniques, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques,

34. *Loi n°2013-1168 du 18 déc. 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JOFR 19 déc. 2013, p.20570.*

35. *Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n°0062 du 15 mars 2011 page 4582, texte n°2.*

36. *Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, J.O. du 6 février 2015 p.1811.*

y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés, ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.
La France anticipe ainsi l'adoption de la future directive « SRI »[37] dont l'objet est de renforcer les capacités nationales des États membres en matière de cybersécurité, notamment par la création d'une autorité nationale de cybersécurité, la coordination européenne en matière de réponse aux incidents et d'instaurer une obligation, pour les administrations publiques et opérateurs de secteurs d'importance critique, de notifier les incidents informatiques significatifs à l'autorité nationale de cybersécurité.

A ces éléments, qui œuvrent à permettre un accès toujours plus important aux données confidentielles, s'ajoutent de nouvelles dispositions visant à permettre la transmission de données de manière automatique, notamment à des fins fiscales. Sur ce point, l'on notera que la loi de séparation et de régulation des activités bancaires[38] a entendu ajouter, au sein du Code général des impôts, l'article 1649 AC, au titre duquel *« les teneurs de compte, les organismes d'assurance et assimilés et toute autre institution financière mentionnent, sur la déclaration visée à l'article 242 ter, les informations requises pour l'application des conventions conclues par la France organisant un échange automatique d'informations à des fins fiscales »*. Cette disposition a pour objet de permettre la mise en œuvre d'accords internationaux en vue de promouvoir l'échange d'informations fiscales dont l'accord « FATCA »[39], qui organise l'échange automatique d'informations fiscales, entre un pays et les États-Unis, représente l'exemple le plus pertinent.

37. *Proposition de directive du parlement européen et du conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union disponible sous le lien : ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666*

38. *Loi n°2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires, JORF n°0173 du 27 juillet 2013 page 12530, texte n°1.*

39. *Voir sur ce point : Actualité Portail de l'Economie et des Finances, Loi «FATCA» : un accord signé entre la France et les Etats-Unis, disponible sous le lien http://www.economie.gouv.fr/signature-accord-fatca.*

6 - MOYENS ET MÉTHODES POUR LA CONFIDENTIALITÉ DES ARCHIVES ELECTRONIQUES

Le droit formalise les obligations en matière de confidentialité, mais impose peu de moyens pour protéger les actifs informationnels, et notamment les archives électroniques.

Ce chapitre développe les bonnes pratiques organisationnelles et techniques qui peuvent être mises en œuvre pour prévenir les risques sur la confidentialité.

6.1 - L'analyse des risques

La problématique de la confidentialité doit être abordée sur une approche risque. Il s'agit de mesurer les risques sur la confidentialité et ceux relatifs à l'accessibilité aux archives. Du point de vue de l'archiviste, celui-ci peut utiliser l'approche risque de l'ISO 30300, et l'informaticien l'approche risque de l'ISO 27005 ou EBIOS. Une méthode combinée permet de clarifier le besoin et de positionner les risques acceptables selon les solutions envisagées.

Les chapitres suivants présentent les défenses à mettre en œuvre pour prévenir les risques sur la confidentialité.

6.2 - Construire un bastion

Pour assurer la confidentialité, le principe de défense en profondeur, inspiré des plans historiques de Vauban, est le concept fondamental de la SSI. Il s'agit de mettre en œuvre un ensemble de remparts qui seront autant de difficulté pour accéder au bastion de conservation des archives numériques par une personne non autorisée.

Ces remparts sont constitués, au niveau de l'architecture technique, de différents domaines réseaux (MZ/DMZ[40]) imbriqués en « oignons » jusqu'au réseau de communication des espaces sécurisés de conservation. Ainsi le réseau ouvert sur internet sera isolé du réseau interne. Au même titre, le réseau des administrateurs sera isolé du réseau interne et du réseau « bastion » de conservation. Chaque porte entre les réseaux est filtrée et contrôlée. Les serveurs doivent s'authentifier pour chaque transaction, supportée par exemple par une PKI[41] ou clé SSH[42].

Les applications communiquent également par transaction via des « paquets » systématiquement contrôlés pour éviter tout risque lié à un accès direct d'un utilisateur à un applicatif sensible, à une base de données ou à un espace de conservation. Il s'agit, dans le jargon de l'informaticien d'une architecture *« n tiers »* dans laquelle, par exemple, il est exclu qu'un utilisateur accède directement à un fichier d'archives. Le type d'architecture est une spécification essentielle lors de l'acquisition d'un composant d'un SAE. Une incompatibilité entre l'application et l'architecture réseaux peut perturber un projet ou induire des risques importants.

---

40. MZ/DMZ (Militarised Zone / Demilitarised Zone) : la MZ est un sous réseau informatique d'un réseau informatique principal et protégé par un pare-feu. La DMZ est un réseau informatique directement exposé aux accès extérieurs (par ex. Internet). La connexion entre ces deux types de zone est garantie et protégée par un (ou plusieurs) pare-feu(s). La séparation MZ/DMZ permet de protéger les serveurs dits « sensibles » (situés en MZ) et de limiter l'accès à une personne non autorisée qu'aux seuls serveurs de la DMZ (serveurs ne contenant aucune donnée sensible).

41. PKI : Public Key Infrastructure ou IGC (Infrastructure de Gestion de Clés)

42. SSH (Secure Shell) : protocole de communication sécurisé par chiffrement des échanges

Enfin, les remparts « logiques » constitués par les différents réseaux et applications seront corrélés aux remparts physiques : l'accès des utilisateurs internes est contrôlé par l'accès aux bâtiments, les administrateurs dans des bureaux cloisonnés avec un deuxième contrôle d'accès, et le Datacenter est lui-même protégé dans une troisième enceinte avec un système d'accès particulièrement sécurisé.

6.3 - Cloisonner les archives et les métadonnées

Le numérique permet dans l'absolu de s'affranchir de toute logique de classement des fichiers, car il suffit de gérer un simple lien entre les métadonnées documentaires et un fichier. Le classement est ensuite reconstitué virtuellement par les métadonnées.

Dans un contexte d'archivage numérique, qui répond à des exigences de sécurité importantes, il convient de cloisonner les espaces de conservation par fonds d'archives, notamment entre les différents propriétaires (pour les tiers archiveurs qui gèrent plusieurs clients, pour les DSI qui gèrent plusieurs filiales, …).

Il s'agit de créer des « domaines » de conservation dans les espaces de conservation, parfaitement étanches, où seront conservés les fonds de chaque entité.

Ce cloisonnement sera indépendant de la description documentaire définie dans les applications, qui permettra un cloisonnement logique, de telle manière qu'un dysfonctionnement ou une attaque de l'applicatif ne permette pas un accès aux domaines voisins.

6.4 - Etanchéifier les moteurs et instruments de recherche

Il est très séduisant d'intégrer des fonctionnalités de moteurs de recherches évolués dans un système d'archivage. Ces moteurs ont la capacité d'indexer de grandes quantités de données et le contenu exhaustif des archives.

Il convient de s'assurer que le moteur de recherche respecte bien les mécanismes d'habilitations existants, de manière à ce que le résultat d'une recherche d'un propriétaire d'archives ne pointe pas vers les documents les plus confidentiels d'un autre propriétaire. De façon identique, toutes les précautions d'usage devront être prises pour éviter l'indexation accidentelle des archives par des moteurs externes.

6.5 - Sécuriser les accès aux archives numériques

La gestion des accès est le nerf de la guerre en matière de confidentialité. Le meilleur système de défense en profondeur ne sert à rien si les accès ne sont pas correctement gérés.
L'accès aux archives numériques doit être vu sous un angle archivistique : le référentiel d'accessibilité est un ensemble de règles structurées de description et d'accès, associé à des profils d'utilisateurs. Cela permettra par la suite d'autoriser les accès d'un comptable aux factures ou d'un gestionnaire RH aux feuilles de paie.

Le travail archivistique est donc préalable à toute acquisition ou paramétrage d'une solution d'archivage numérique. Il s'agit de définir les besoins d'accessibilité pour vérifier que les

fonctions de paramétrage et d'administration sont bien adaptées. Un paramétrage mal calibré risque de trop « ouvrir » les fonds, et d'augmenter le risque sur la confidentialité, ou, à l'inverse, de trop « fermer » les fonds, auquel cas la valeur ajoutée de la solution pourrait être remise en cause par les utilisateurs qui reviendraient alors à leurs dossiers suspendus ou à des fichiers sur disques durs.
Enfin, l'authentification de l'utilisateur est une composante essentielle pour la confidentialité, comme pour tout système d'informations. La robustesse des mots de passe doit être conforme à une politique de gestion des mots de passe formalisée et prévoir des fonctionnalités de révocation opérationnelles. Une authentification basé sur les seuls « identifiant + mot de passe » présente un risque, car l'utilisateur lui-même est considéré comme le maillon faible et peut divulguer ses informations d'accès. Pour l'accès à des fonds particulièrement sensibles, des solutions d'authentification double facteur, peu contraignantes pour l'utilisateur, existent sur le marché et apportent un réel gain de sécurité.

6.6 - Le besoin d'en connaître des fonctions supports

Pour autoriser un utilisateur à accéder à un type de document, il est nécessaire d'avoir un administrateur et pour autoriser un administrateur : il faut donc un super-administrateur. Ces privilèges de super-administration sont à surveiller avec attention car, même si un tel administrateur ne dispose d'aucun privilège d'accès aux archives, il peut se créer en tant qu'utilisateur fictif pour contourner les restrictions de droits. Une fonction d'historisation (journalisation des événements) des transactions réalisées par ce type d'administrateur est fortement préconisée. Ce journal ne doit pas être modifiable par ces mêmes administrateurs ou super-administrateurs, et devra être surveillé par une entité indépendante des fonctions d'administration.
On peut signaler à cet égard que la norme NF Z 42-020 de 2012, relative au composant coffre-fort numérique, intègre l'exigence suivante : les administrateurs techniques ou les administrateurs fonctionnels ne peuvent pas avoir accès aux objets numériques déposés dans les coffres forts des utilisateurs.
Le positionnement de l'administrateur est important : s'il est archiviste et qu'il peut accéder à l'ensemble du fonds, les restrictions de privilèges seront moindres que s'il s'agit d'un administrateur de la DSI, par exemple, qui n'a pas le besoin d'en connaître.
Dans le cas d'une externalisation chez un tiers archiveur, il est pertinent de disposer d'une console d'administration client, de telle sorte que le tiers archiveur ne puisse pas autoriser son propre personnel à accéder aux fonds d'archives sans que leurs propriétaires en soient informés.
Si nécessaire, il convient que le client habilite un exploitant du tiers archiveur, nominativement identifié, pour des besoins de support ou de prestations particulières.
Cette fonction est importante pour rassurer le client, mais également pour protéger le tiers archiveur par un report de responsabilité clairement formalisé dans le contrat d'archivage numérique.

6.7 - La traçabilité

La traçabilité d'accès aux archives, préconisée par la norme NF Z42-013, permet de démontrer qu'aucun utilisateur non autorisé n'a accédé aux documents.

7 - LE CHIFFREMENT DANS UNE SOLUTION D'ARCHIVAGE NUMÉRIQUE

Le chiffrement est un procédé consistant à rendre une information inintelligible par toute personne ou système technique ne possédant pas la « clé » nécessaire pour la déchiffrer.
Ce procédé permet, qu'en cas d'accès non autorisé à une information, celle-ci ne soit pas exploitable sans connaître la clé de déchiffrement[43]. Le chiffrement ne protège donc pas contre l'accès à l'objet d'archive, mais empêche l'exploitation des informations contenues dans cet objet.

L'objectif du chiffrement est de renforcer la confiance en se protégeant contre deux types de menaces principales :

- **Menaces extérieures à une entité** : il s'agit de prévenir les impacts en cas d'interception, détournement ou vol de données sensibles par une entité malveillante ou indiscrète, notamment lorsque les données sont particulièrement exposées. Il s'agit par exemple :
  - de l'interception d'un transfert de données sur internet par un hacker ;
  - de la surveillance étatique massive, indifférenciée et non contrôlée ;
  - etc.
- **Menaces intérieures à une entité** : il s'agit de protéger les informations sensibles de deux types de populations :
  - Les utilisateurs internes non habilités, non assujettis au secret professionnel ou au « besoin d'en connaître » d'informations particulièrement sensibles[44] ;
  - Les opérateurs techniques disposant de privilèges élevés permettant de contourner les systèmes de gestion des droits d'accès aux informations (personnel d'un tiers archiveur, administrateur et exploitant informatiques d'une DSI, …).

C'est cette dernière population (les opérateurs techniques) qui est particulièrement concernée par la tendance de fond qui vise à protéger les données sensibles, car la frontière qui sépare l'intérieur et l'extérieur de l'organisme s'estompe du fait :

- de l'externalisation ou de la mutualisation des services d'exploitations informatiques internes ;
- de l'usage d'infrastructures externalisées sur des Datacenters externes (*Cloud*) ;
- du développement des services en mode hébergé (SaaS).

Il est important de noter que le chiffrement permet de protéger les informations sensibles du fait que le secret (la clé de déchiffrement) est maîtrisé par une sphère de confiance limitée aux populations concernées par le « besoin d'en connaître ». Toutefois, le chiffrement n'apporte aucune sécurité complémentaire si le secret n'est pas réellement maîtrisé ou si les clés sont détenues par ces mêmes opérateurs techniques.

Par analogie, la serrure de la chambre d'hôtel ne protège pas complètement le client car le personnel possède un « pass » d'accès pour l'ensemble des chambres. La sécurité du client repose sur la confiance qu'il accorde au personnel de l'hôtel.
Les opérateurs de services sont actuellement peu transparents sur les moyens mis en œuvre

43. Cela induit qu'en cas de perte de la clé, l'information restera inintelligible.

44. Cet objectif de sécurité est traité par la gestion des identités et des accès développé dans le concept de défense en profondeur (Cf. chapitre 6 - Moyens et méthodes pour la confidentialité des archives électroniques

pour le chiffrement et la protection des clés en particulier. Un bon nombre affiche un chiffrement des informations des clients tout en détenant une seule clé, connue de l'opérateur uniquement, permettant de déchiffrer l'ensemble des informations contenues dans le système d'information.

Il s'agit là du véritable dilemme des technologies de chiffrement : la complexité du chiffrement nécessite des compétences d'opérateurs techniques pointues, alors qu'un des objectifs du chiffrement est justement de se protéger de ces mêmes opérateurs.

L'enjeu n'est pas tant de savoir comment chiffrer une archive électronique, mais de savoir gérer les clés de chiffrement et de déchiffrement. Cela nécessite l'usage de technologies, mais également une organisation bien pensée.

Le chiffrement constitue clairement une barrière supplémentaire envisageable dans un système de défense en profondeur. Cette option est réalisable si l'analyse de risque identifie une vulnérabilité sur des archives particulièrement sensibles, si un texte de référence le préconise (par exemple pour le label coffre-fort numérique du particulier de la CNIL[45]) ou si une réglementation l'impose (par exemple les jeux en ligne).

Ce guide ne traite pas des technologies de chiffrement, largement documentées par ailleurs[46], mais de l'application du chiffrement au domaine de l'archivage électronique.

Le domaine d'application du chiffrement est potentiellement vaste et techniquement complexe, car l'archive électronique est un composite de données et de métadonnées, hébergées dans un système d'archivage électronique composé lui-même de différentes chaînes matérielles et applicatives.
Dans un premier temps, **le périmètre d'application du chiffrement** dans une solution d'archivage électronique sera précisé avec, ensuite, une présentation des cas d'usage pour les transferts et la conservation des archives électroniques.

Le chiffrement durant la conservation des archives sera particulièrement développé selon deux axes :

- **Comment chiffrer pendant la période de conservation et comment gérer les secrets ?** Le chiffrement peut s'appliquer sur les différents éléments qui constituent l'objet d'archives (document, métadonnées, …). Les différents composants du système d'archivage électronique peuvent être amenés à chiffrer. La gestion des clés peut être réalisée au niveau le plus bas (le composant de stockage) jusqu'au plus haut (l'utilisateur humain). Les cas d'usages les plus significatifs seront précisés dans cet axe.
- **Quels impacts sur la gestion du cycle de vie des archives ?** L'usage du chiffrement des objets d'archives et/ou des métadonnées associées a un impact sur la gestion de l'accessibilité (indexation), de l'intégrité et de la pérennité. Il est important d'anticiper ces contraintes pour réaliser le choix le plus pertinent lorsqu'il est nécessaire de chiffrer.

45. http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20140207&numTexte=76&pageDebut=&pageFin

46. Pour faciliter la lecture de ce chapitre, nous recommandons de consulter la littérature sur les technologies de chiffrement, notamment sur le site de l'ANSSI ainsi que sur les concepts fondamentaux de l'archivage électronique formalisés dans OAIS et NF Z 42-013.

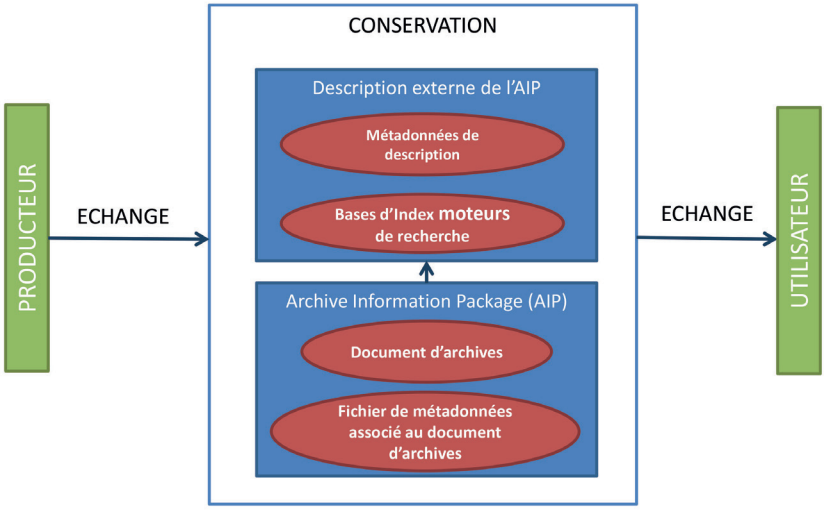
7.1 - Où sont les données à protéger ?

L'exposition des archives n'est pas la même lors des **échanges** et pendant la **conservation**. L'échange (pour le versement, la consultation et la réversibilité), lorsque les archives transitent via des réseaux partagés, nécessitera plus de moyens pour la confidentialité que pendant la conservation, notamment si les espaces de conservation sont peu exposés.
Pour la conservation des archives numériques, deux périmètres d'application potentiels du chiffrement peuvent être identifiés :

- le document d'archive lui-même ;
- ses métadonnées associées. Les métadonnées peuvent être conservées sous plusieurs formes :
    - en base de données ;
    - dans des fichiers associés aux fichiers d'archive ;
    - dans les journaux et les traces ;
    - dans des moteurs de recherches et autres instruments de recherche.

Le schéma ci-dessous est une application du modèle OAIS[47], dont l'un des concepts majeurs est de rendre indépendant l'objet d'archives de tout système d'information pour en assurer la pérennité.

Un SAE gère de manière différenciée les métadonnées et le document d'archive dans un composant de conservation. Les métadonnées peuvent-être injectées dans un système documentaire pour des besoins d'accessibilité et de recherche.



La donnée à protéger est donc potentiellement dans plusieurs endroits différents pour lesquels il existe différentes approches pour la confidentialité.

47. *OAIS - Open Archive Information System*

7.2 - Le chiffrement des communications

7.2.1 - La communication numérique des archives

Lors de la consultation d'une archive électronique, les informations échangées entre un utilisateur et une solution d'archivage électronique sont particulièrement exposées aux risques d'interception, notamment lorsqu'elles transitent par Internet.

Un chiffrement des communications est ici clairement recommandé, par exemple avec l'usage de protocoles comme HTTPS, qui intègre les logiques de chiffrement SSL ou TLS dans leurs versions en vigueur. Cette technologie est couramment employée par les DSI et ne pose aucune difficulté particulière d'implantation[48].

Une vigilance particulière est à apporter à la conformité des paramétrages de cette technologie[49] et à ses possibilités de contournement. Des tests de pénétration réguliers, réalisés par des cabinets spécialisés, sont recommandés. De plus, une veille sécuritaire associée à des mises à jour régulières des logiciels permettra de prendre en compte, si nécessaire, les alertes de sécurité concernant les briques technologiques qui implémentent ces protocoles.

7.2.2 - Les transferts « de masse « d'archives numériques

Il s'agit de transactions de versement ou de restitution de lots d'archives.
Au même titre que la communication, les transferts de masse entre un système d'informations et une solution d'archivage électronique doivent être chiffrés quand ceux-ci transitent par des réseaux non sécurisés (Internet, par exemple) pour prévenir toute interception. Le transfert doit également intégrer une gestion de l'intégrité des échanges.

De nombreuses solutions du marché proposent des produits adaptés à ce besoin. Une convention de transfert doit être établie entre les parties communicantes sur les technologies à employer.

Le cas échéant, un transfert sur media amovible, pouvant lui-même être sécurisé, sera privilégié par rapport à une télétransmission non chiffrée.

7.3 - Le chiffrement pendant la durée de conservation

Si les principes de défenses en profondeur et de gestion des accès sont correctement implantés, les archives numériques disposent d'un niveau de protection important face aux attaques extérieures.

Un chiffrement pendant la durée de conservation permet une protection supplémentaire des archives, notamment face aux risques internes.

---

48. Pour plus de recommandation, consultez notamment les Guides et recommandations téléchargeables sur le site de l'ANSSI : http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides.

49. Cf. notamment les documents suivants de l'ANSSI : « mécanismes cryptographiques : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » et « SSL/TLS : état des lieux et recommandations »

Si une solution de chiffrement est envisagée, une étude de conception par un expert est nécessaire pour mettre en œuvre le niveau de robustesse adapté aux risques. L'ANSSI a publié des règles et recommandations concernant le choix et le dimensionnement des mécanismes de sécurité[50] ainsi que des recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques[51].

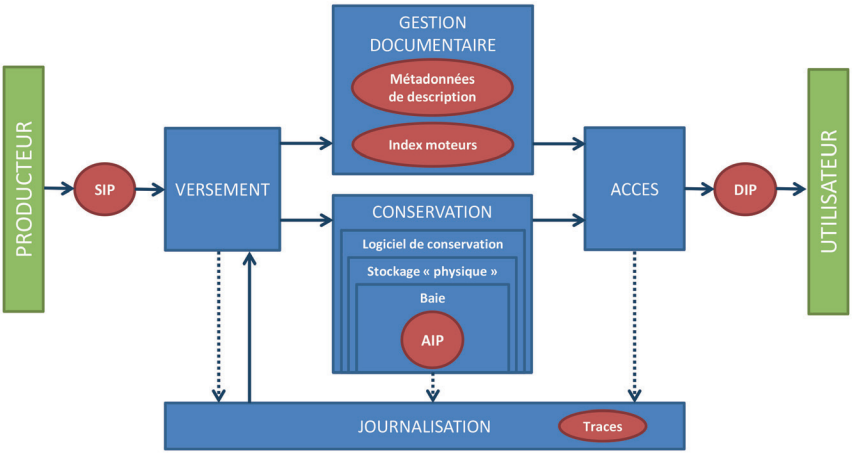
Ce Guide présente un exemple d'implémentation adapté à la problématique spécifique de l'archivage.
L'architecture des mécanismes cryptographiques intégrés dans un SAE dépendra de différents choix :

- le positionnement des mécanismes cryptographiques (matériels ou logiciels) dans les composants du SAE ;
- la granularité de chiffrement (au document, catégorie de document, propriétaire ou fonds d'archives) ;
- le type de chiffrement (symétrique ou asymétrique) ainsi que les modalités de gestion des clés.

7.3.1 - Les composants d'une solution d'archivage numérique

Le chiffrement peut être implanté sur chacun des composants utilisés pour accéder à un fichier d'archives numérique.

Les paragraphes suivants rappellent quels sont les composants d'une solution d'archivage[52] numérique pour identifier ensuite où positionner les mécanismes de chiffrement et de déchiffrement.



50. *Annexe B1 du RGS : http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf*
51. *Annexe B2 du RGS http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B2.pdf*
52. *Ce schéma s'inspire du modèle OAIS. SIP : paquet d'information à verser ; AIP : paquet d'information archivé ; DIP : paquet d'information diffusé.*

7.3.1.1 - Composants de stockage « Physique »

L'enregistrement physique d'un fichier d'archives est réalisé sur un support de type disque magnétique ou mémoire rapide.

Dans un environnement professionnel, les archives sont généralement conservées dans des baies de stockage. Une baie est composée d'un ensemble de supports physiques de stockage (disques magnétiques, mémoires) pilotés par la baie selon une norme RAID (5 ou ultérieure).
Pour illustrer le principe de fonctionnement d'une telle baie, chaque fichier est fractionné en « petits » morceaux répartis sur les différents supports de la baie de telle sorte qu'en cas de défaillance de l'un des supports, il n'y ait pas de perte du fichier. Le contenu du nouveau support est automatiquement reconstitué par le mécanisme RAID. L'application qui pilote la baie gère l'allocation des zones de stockage de chaque partie de fichier et l'intégrité de l'ensemble de l'espace de conservation.

7.3.1.2 - Composants logiciel de conservation

Les applications logicielles de conservation (type coffre-fort numérique) constituent une « surcouche » logicielle qui gère principalement la traçabilité et l'intégrité des objets numériques contenus dans une ou plusieurs baies.

Selon les architectures de SAE, les composants de journalisation sont intégrés au composant coffre-fort numérique.[53]

7.3.1.3 - Composants de gestion documentaires et d'accès

Il s'agit de l'interface homme/machine entre un utilisateur et le SAE. Ces composants gèrent trois fonctions principales :

- le cycle de vie des archives ;
- la description, le classement et les instruments de recherches associés ;
- les fonctions d'accès intégrant l'authentification au système ainsi que les droits et privilèges des utilisateurs.

53. Cf. NFZ 42-020 pour la définition des fonctionnalités coffre-fort numérique.

7.3.2 - Positionnement du chiffrement

7.3.2.1 - Chiffrement par le composant de stockage

L'application qui pilote la baie peut intégrer des fonctions de chiffrement qui peuvent être activées, soit pour la baie en général, soit pour une « partition virtuelle » de cette baie qui peut correspondre à un domaine d'archives à protéger. Cette option protégera les fonds contre un vol de la baie en entier (si la clé est externe à la baie), ce qui est peu probable si les règles de sécurité physique du Datacenter sont respectées. Il est à noter que ce dispositif protège peu d'une intrusion directe dans le réseau ou d'un accès direct à la baie par un exploitant technique, car celui-ci accédera aux données stockées dans la baie via l'application pilote, qui assure, par là-même, ce chiffrement.

7.3.2.2 - Chiffrement par le composant logiciel de conservation

Un chiffrement contrôlé au niveau du composant logiciel de conservation permet d'empêcher la lecture en clair des informations contenues dans la baie par les opérateurs du composant de stockage et/ou de se protéger d'une éventuelle intrusion réseau qui permettrait d'accéder à l'application pilote des baies de conservation.

Cette solution ne protège pas l'accès aux archives par les exploitants techniques du coffre-fort numérique qui auraient alors accès aux clés (ou au mécanisme qui les exploitent). Dans l'exemple de la conservation des transactions des jeux en ligne, cette technique est utilisée avec détentions des clés de déchiffrement par l'autorité de régulation.

Cette méthode permet, par exemple, de se protéger contre les intervenants d'un opérateur Cloud quand ce dernier n'assure qu'un service de mise à disposition de capacités de stockage.

7.3.2.3 - Chiffrement par le composant de gestion documentaire et d'accès

Un chiffrement géré au niveau de l'application de gestion documentaire et d'accès protégera les données des administrateurs du coffre-fort numérique et des composants sous-jacents. Cette solution ne protège pas l'accès aux archives par les exploitants techniques de ce composant si la clé de déchiffrement est gérée par le composant lui-même.

Ces trois choix de positionnement sont volontairement limités dans ce Guide pour présenter les principes structurants. En réalité, les mécanismes de chiffrement peuvent être des fonctions intégrées à un composant ou connexes à un ou plusieurs composants. Dans un choix hybride, il peut être envisagé un composant dédié à la gestion des mécanismes cryptographiques interfacé avec d'autres composants.

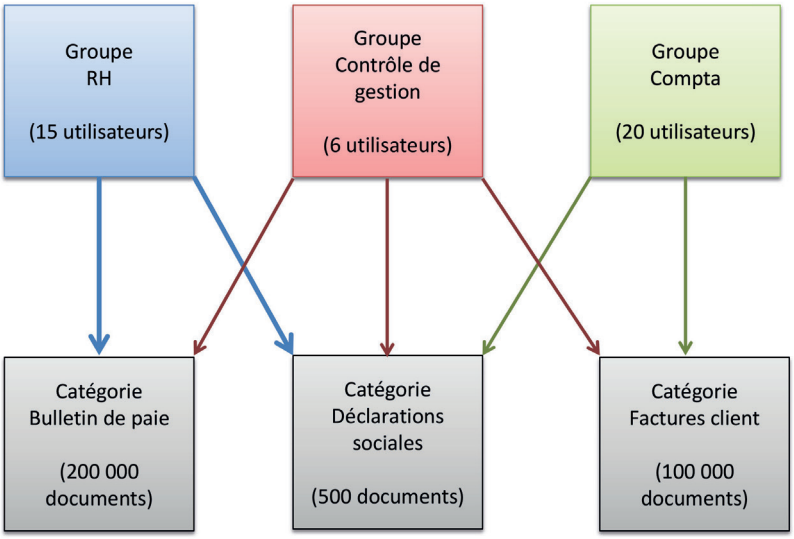
7.3.3 - Niveau de granularité du chiffrement

Indépendamment du positionnement du moyen de chiffrement choisi, il convient de définir comment organiser le déchiffrement.

Le choix du niveau de granularité du chiffrement est important dans une configuration SAE pour une entreprise ou une administration, car plusieurs centaines d'utilisateurs accèdent de manière différenciée à des fonds pouvant contenir des millions de documents.

Il s'agit de la problématique d'un SAE pour une organisation en environnement B to B développée dans ce Guide.

Exemple d'organisation documentaire dans un contexte B to B :



Ce schéma représente un usage traditionnel de gestion des accès où le système d'administration du SAE permet de gérer des groupes fonctionnels d'utilisateurs. Un utilisateur affecté à un groupe fonctionnel pourra accéder aux catégories de documents de ce groupe. Par exemple, un utilisateur affecté au groupe RH pourra accéder aux feuilles de paie et aux déclarations sociales, mais en aucun cas aux factures clients.

Dans ce modèle, il existe trois niveaux de granularités possibles :

- **granularité de niveau 1 (générale)** : déchiffrement avec une clé pour l'ensemble des fonds (dans l'exemple, *a minima*, cela nécessite une clé) ;
- **granularité de niveau 2 (catégorie)** : déchiffrement avec une clé par catégorie de documents (dans l'exemple, cela nécessite trois clés) ;
- **granularité de niveau 3 (document)** : déchiffrement avec une clé par document (dans l'exemple, cela nécessite plus de 300 000 clés).

Le choix d'un niveau de granularité du chiffrement, *a minima*, à la catégorie de document permet :

- de différencier le niveau de sécurité pour les documents sensibles et ceux qui restent en clair pendant la conservation
- de renforcer et rendre indépendants les secrets par propriétaire d'archives. En cas de réversibilité d'une catégorie pour un propriétaire, celui-ci n'aura pas à connaître les « secrets » des autres propriétaires.

L'indépendance des fonds est particulièrement importante pour les tiers archiveurs qui gèrent par nature des environnements multi-clients.

7.3.4 - Technologies de chiffrement

Deux technologies sont usuellement exploitées :

- **le chiffrement symétrique** : la même clé permet de chiffrer et de déchiffrer. Cette technologie présente l'avantage de nécessiter peu de puissance de calcul. Sa contrainte est que la clé doit rester secrète ;
- **le chiffrement asymétrique** : Il s'agit de générer une clé publique permettant de chiffrer les archives ainsi qu'une clé privée permettant de les déchiffrer. Le mécanisme assurant le chiffrement ne connaît pas le « secret » pour déchiffrer (et réciproquement). La contrainte est que cette technologie demande une plus grande puissance de calcul.

L'usage courant combine les deux technologies : il s'agit, dans l'exemple d'échange sécurisé de type SSL, de chiffrer un objet à échanger avec une clé symétrique, puis de chiffrer/déchiffrer la clé symétrique avec la clé publique d'un chiffrement asymétrique pour sécuriser l'échange des secrets, avant la communication de l'objet.

Dans le cadre du chiffrement d'un fonds d'archives pendant la conservation, où la volumétrie est importante, un chiffrement asymétrique de l'ensemble des fonds nécessiterait des moyens considérables.

L'usage du chiffrement symétrique pour protéger les objets d'archives pendant la période de conservation, associé à un mécanisme de protection de clés basé sur un chiffrement asymétrique, semble une solution raisonnable à l'heure actuelle compte tenu de l'état des technologies et de la performance des algorithmes de chiffrement usités.

Il est à noter que lors d'un échange chiffré d'objet numérique, la clé symétrique est générée au moment de l'échange et seul le couple émetteur/destinataire disposera de cette clé. **Celle-ci n'est utile que durant la session d'échange.** Pour la session d'échange suivante, une nouvelle clé symétrique est générée et échangée. De cette manière, en cas de divulgation de la clé, celle-ci ne sera plus exploitable lors des sessions d'échange suivantes.

A contrario, dans une application du chiffrement pendant la conservation, **la clé symétrique est utile et nécessaire durant toute la durée de conservation**, car c'est cette même clé qui est utilisé pour déchiffrer les archives en cours de conservation[54].

---

54. Notons que quel que soit la technologie de chiffrement choisie, les clés sont uniques pour un objet chiffré. Il n'est pas possible de générer plusieurs clés de chiffrement ou déchiffrement pour un même document.

Ceci induit des risques importants en cas de divulgation de la clé et caractérise la problématique spécifique du chiffrement des archives pendant leur conservation. Dans ce contexte, la protection des clés est particulièrement importante, car il s'agit de protéger durablement un ensemble important d'informations sensibles.

A noter que la qualité des clés produites pour le chiffrement et/ou pour la PKI est un enjeu fort de sécurité. En effet, il ne sert à rien de compliquer la solution d'archivage avec du chiffrement si la robustesse des clés mises en œuvres est faible et qu'elles peuvent être cassées rapidement. L'utilisation d'un module matériel de sécurité (HSM[55]) pour la réalisation de ces fonctions est fortement préconisée et/ou obligatoire dans le RGS, selon la nature du composant concerné (application ou PKI).
Dans ce cadre, un équipement dont la sécurité a été évaluée par un laboratoire, voire certifié[56] ou qualifié[57], est conseillé, parce que les fonctions les plus sensibles, telles que le générateur aléatoire, ont fait l'objet de tests et de contrôles.

Par ailleurs, la gestion des clés par une PKI permettra de définir et de contrôler l'ensemble des processus associés à la gestion du cycle de vie et à la protection des clés. Par exemple, la PKI permettra de garantir que les clés de chiffrement ne sont jamais utilisées en clair dans un logiciel, mais toujours exploitées dans le HSM et/ou dans la carte à puce de l'utilisateur. De plus, l'utilisation d'un HSM permet de structurer la création initiale des clés dans le cadre d'une cérémonie des clés. Lors de cette cérémonie, les clés les plus importantes de la solution doivent être générées et sauvegardées dans des formats pérennes afin d'en garantir la disponibilité à long terme.

Focus : HSM ou Hardware Security Module

Un HSM est un module matériel de sécurité. Cet équipement fonctionne en coprocesseur d'un autre équipement informatique. Il délivre à ce dernier un ensemble de fonctions cryptographiques telles que des algorithmes symétriques (DES, AES,..), des algorithmes asymétriques (RSA, ECDSA,…), des fonctions de calcul d'empreintes (SHA-1, SHA-2,…), des fonctions de tirage et de diversification de clés (liste non exhaustive).

Une fonctionnalité importante d'un HSM consiste à protéger les clés aux différents moments de leur cycle de vie : depuis leur création jusqu'à leur suppression, en passant par leur utilisation. De plus, les mécanismes proposés par le HSM doivent permettre d'assurer la sauvegarde et idéalement l'exportation sécurisées des clés, pour en garantir la disponibilité dans le temps.

Un HSM peut se présenter sous la forme d'un équipement réseau (« appliance ») ou sous la forme d'une carte add-on qui s'intègre dans un bus d'un serveur. Les services d'un HSM sont disponibles au travers d'une API (Application Programming Interface) propriétaire, différente d'un constructeur à l'autre, ou standardisée, comme l'interface PKCS#11 par exemple.

55. HSM : Hardware Security Module

56. Cf. Certification selon une méthode adaptée au domaine concerné par exemple la méthode des critères communs.

57. Dans le RGS, l'ANSSI définit trois niveaux de qualification : élémentaire, standard et renforcé .

Un HSM met en œuvre des mécanismes matériels de sécurité : détection d'intrusion, détection de mouvement, effacement des clés, surveillance des tensions et des températures. Il met aussi en œuvre des mécanismes logiciels de sécurité : identification du logiciel, vérification d'intégrité du logiciel, autotest …

C'est dans le cadre d'une évaluation sécuritaire qu'un laboratoire indépendant désigné par le fabricant vérifie les mécanismes de protection et les fonctions de sécurité du HSM. Les méthodes d'évaluation couramment utilisées pour évaluer un produit de sécurité sont le FIPS établi par le NIST (organisme nord-américain) et les Critères Communs, normalisés par l'ISO (ISO 15408) et reconnus par les principaux pays occidentaux.

7.3.5 - Qui doit détenir les clés de chiffrement et de déchiffrement ?

Dans le cas d'un usage SAE où un groupe d'utilisateurs peut accéder à un ensemble de documents, il est nécessaire d'exploiter la clé de déchiffrement au moment de la consultation. Plusieurs méthodes sont réalisables pour chiffrer et déchiffrer, par exemple :

- **Méthode 1** : l'utilisateur ou un système tiers interfacé avec le SAE assure les fonctions de chiffrement et déchiffrement ;
- **Méthode 2** : le SAE transmet la clé à l'utilisateur qui réalisera ensuite le déchiffrement pour consulter le document ;
- **Méthode 3** : le SAE déchiffre le document avant envoi pour consultation.

La méthode 1 consiste à opérer le chiffrement et déchiffrement par l'utilisateur ou un système tiers dans son propre environnement de confiance. Dans ce cas, le SAE n'a vocation qu'à assurer l'intégrité d'un objet numérique non lisible. Il s'agit d'une application coffre-fort numérique, sans fonction de chiffrement. Avec cette méthode, la responsabilité de la protection des clés incombe à l'utilisateur.

La méthode 2 nécessite de distribuer l'ensemble des clés permettant de déchiffrer chaque document à une population habilitée pour les consulter. Ceci signifie que les clés sortent de la sphère de confiance du SAE. Cela nécessite de mettre en œuvre des mécanismes de protection, de génération et régénération de clés particulièrement robustes et fiables sur du très long terme. Ce type d'architecture sera généralement intégré dans des sphères de confiance plus larges comme, par exemple, dans le secteur de la défense où plusieurs sphères existent pour l'échange des documents classifiés.

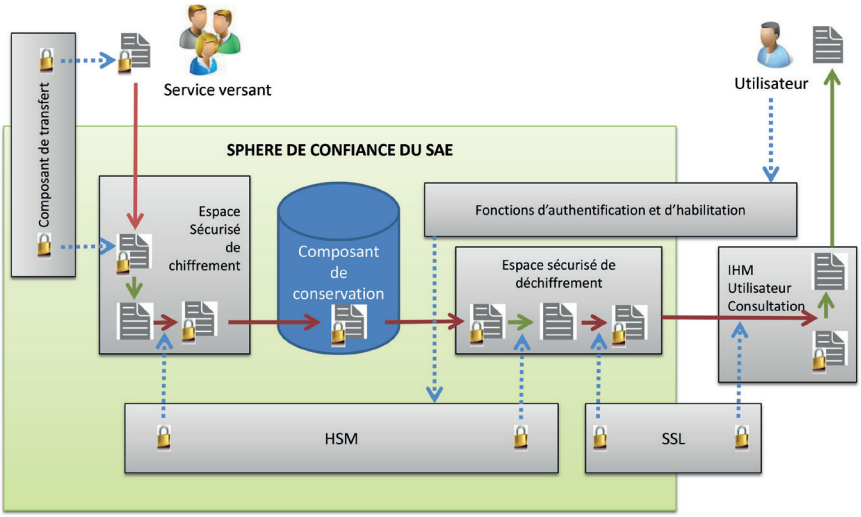
Ce guide développe la méthode 3, qui présente les avantages de maintenir les « secrets» dans une sphère de confiance constituée par le SAE et d'être « industrialisable ». Il ne s'agit pas d'une préconisation d'architecture, mais d'un cas d'usage développé à fin pédagogique pour illustrer un exemple d'architecture.

La méthode 3 consiste à déchiffrer l'objet d'archive en sortie de son environnement de conservation puis à le transmettre de façon sécurisée (via un chiffrement SSL ou TLS) pour sa communication. Ce deuxième chiffrement pour communication est adapté à une transaction « un à un », au moment de la communication uniquement. La clé (SSL ou TLS) utilisée pour la communication est temporaire est différente de la clé utilisée dans l'environnement de conservation.

7.3.6 - Exemple d'architecture d'un SAE intégrant un chiffrement durant la conservation

L'exemple d'architecture représenté dans le schéma ci-dessous reprend en partie les concepts de ce Guide avec les choix suivants :

- positionnement des mécanismes cryptographiques au niveau du composant documentaire et d'accès (cf. § 7.3.2.3 -) ;
- niveau de granularité à la catégorie de document ;
- chiffrement symétrique durant la conservation.



Versement

Le document d'archives est versé via un outil de transfert sécurisé assurant le chiffrement temporaire pendant les temps de la communication vers le SAE (Cf. § 7.2.2).

Le document est déchiffré par le composant de transfert puis chiffré par le SAE selon la clé symétrique correspondant à la catégorie de document concerné. Cette clé est conservée dans le HSM et n'est donc pas accessible à un opérateur humain. La clé symétrique est elle-même chiffrée (par un chiffrement asymétrique) pour son transfert vers l'espace sécurisé de chiffrement. Ce dernier déchiffre la clé symétrique (via un déchiffrement asymétrique) pour un usage de chiffrement des nouvelles archives à protéger.

Le document ainsi chiffré est versé dans le composant de conservation et le restera tant que nécessaire.

Consultation

Au moment de la consultation, l'utilisateur s'authentifie via l'IHM[58] [59] du SAE. Le SAE contrôle l'autorisation de consultation sur la catégorie de document concerné et valide l'usage de la clé de déchiffrement par le composant de déchiffrement.
Le composant de déchiffrement négocie l'échange de clé symétrique de la catégorie de document avec le HSM. Le transfert des clés est sécurisé par un chiffrement asymétrique de la clé symétrique de la même manière que pour les versements. Pour sécuriser les échanges vers l'utilisateur, l'espace sécurisé déchiffre le document (avec la clé symétrique de conservation) puis l'envoie vers l'utilisateur via un protocole de communication sécurisé (comme HTTPS sécurisé par une couche SSL ou TLS, avec une autre clé symétrique générée et dédiée pour ce type de transport).

L'IHM de l'utilisateur déchiffre le document pour un affichage dans l'IHM ou un téléchargement. Selon ce schéma, le document est *in fine* accessible en clair par l'utilisateur qui pourra assurer sa diffusion sans aucune protection. S'il est nécessaire de protéger le document pendant et après sa consultation, l'IHM devra intégrer des fonctions de bridage du téléchargement et d'impression, de chiffrement ou suppression des éléments téléchargés dans le cache, ou proposer un mécanisme de chiffrement complémentaire pour la protection des diffusions.

7.3.7 - Moyens de contournement des sécurités cryptographiques

Les architectures de chiffrement induisent généralement l'existence d'un mécanisme liant la gestion des droits d'accès et la gestion des clés. Si la sécurité de l'authentification utilisateur et les principes de défense en profondeur présentés précédemment ne sont pas respectés, il sera possible de contourner l'ensemble des mécanismes de chiffrement.

Ainsi, un opérateur ayant le droit d'administration sur les fonctions d'accessibilité pourra se créer en tant qu'utilisateur et ainsi consulter l'ensemble des fonds sans avoir besoin d'aucune clé de déchiffrement.

A ce titre, et comme évoqué dans le chapitre sur la défense en profondeur, la gestion sécurisée des accès est un préalable indispensable à la mise en œuvre de mécanismes cryptographique. Cela nécessite de :

- sécuriser l'authentification de l'utilisateur par l'usage d'un mécanisme fiable (certificats, mot de passe à usage unique, …) ;
- clairement segmenter les rôles d'administration des fonctions d'accessibilité des rôles d'exploitation technique du SAE ;
- tracer et auditer de manière fine toute transaction d'administration sur les fonctions d'accessibilité afin d'identifier toute tentative de contournement des mécanismes cryptographiques ;
- ne jamais permettre l'accès aux clés de chiffrement aux opérateurs humains ;
- s'assurer que chaque communication de clés est réalisée de manière chiffrée, y compris pour les transactions entre les composants internes d'un SAE.

---

58. IHM : Interface Homme Machine. portail SAE en mode SaaS ou client lourd installé sur le poste de travail de l'utilisateur final.

59. L'authentification de l'utilisateur peut être simple (via seulement un identifiant/mot de passe) ou forte (par l'utilisation conjointe de deux ou plusieurs des éléments suivants : a) identifiant/mot de passe ; b) carte à puce, token, PDA, smartphone ; c) empreinte digitale, structure osseuse du visage, biométrie ; d) géolocalisation.

7.3.8 - Prévention des pertes des clés

Le chiffrement présente un risque sur la pérennité des archives en cas de perte des clés, notamment dans le cas de la détention du secret par l'utilisateur, mais également, dans une moindre mesure, dans le cas d'un chiffrement applicatif.

Il conviendra de mettre en œuvre des procédures de secours, par exemple avec un séquestre de clés chez un tiers de confiance.

Focus : la CNIL et le chiffrement du coffre-fort numérique du particulier

La CNIL a formalisé sa doctrine en matière de service de coffre-fort numérique pour le particulier dans deux textes successifs :

La Délibération n°2013-270 du 19 septembre 2013 portant recommandation relative aux services dits de « coffre-fort numérique ou électronique » destinés aux particuliers. La Délibération n°2014-017 du 23 janvier 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de services de coffre-fort numérique.

Pour la CNIL, le contenu d'un coffre-fort numérique doit être sous le contrôle exclusif de l'utilisateur et, le cas échéant, des personnes mandatées par ce dernier. Ainsi, le fournisseur d'un service de coffre-fort numérique ne doit pas être en mesure d'accéder aux données.

Le respect de cette exigence passe par le chiffrement des documents archivés dans le coffre-fort numérique, mais aussi des métadonnées associées à ces documents. Les métadonnées concernées par l'exigence de chiffrement sont celles qui sont créées par l'utilisateur comme, par exemple, le nom du fichier.

A la différence d'un SAE qui nécessite qu'un ensemble d'utilisateurs accède à un ensemble de documents, un coffre-fort pour un particulier est dans une relation d'un seul utilisateur accédant à ses propres documents. Il est donc envisageable de faire gérer les clés par l'utilisateur lui-même. Dans le référentiel du label, la CNIL précise tout de même que *« lorsqu'un coffre-fort numérique a vocation à conserver des données à long terme, une copie de sauvegarde de la clef de déchiffrement doit être confiée à un tiers de confiance, afin de permettre à l'utilisateur d'accéder à ses données en cas de perte de sa clef. Toute utilisation d'une sauvegarde de la clef de déchiffrement doit faire l'objet d'une traçabilité et d'une information de l'utilisateur concerné ».*

Le recours au chiffrement pour les services de coffre-fort numériques procure un niveau de confidentialité supplémentaire, mais il fait naître des contraintes et des limites, d'une part pour les fonctionnalités de recherche, et d'autre part, pour celles de partage.

7.4 - Chiffrement de la conservation et cycle de vie des archives numériques

L'implantation de technologies de chiffrement pour une solution d'archivage numérique, en particulier, induit un ensemble de considérations archivistiques à prendre en compte pour la gestion de l'intégrité, de l'accessibilité et de la pérennité des archives.

7.4.1 - Les empreintes pour l'intégrité doivent-elles être calculées avant ou après le chiffrement ?

Les empreintes, issues d'algorithmes cryptographiques appliqués à un fichier d'archive, sont la base des garanties d'intégrités spécifiées dans la norme AFNOR NF Z42-013. Le système de journalisation associé à la gestion des empreintes confère une « vocation probatoire » aux archives numériques.

Le chiffrement d'une archive modifie son empreinte, puisque que le fichier chiffré n'est pas le même que le fichier non chiffré. Le fait de calculer une empreinte, puis de chiffrer le fichier d'archive, rend impossible les contrôles d'intégrité sans détenir la clé de déchiffrement pour réaliser le contrôle. Cela posera donc soit un problème conceptuel pour la conformité à la NF Z42-013, soit, dans le cas de la détention des clés par l'utilisateur, une nécessité de partage du secret avec le mécanisme de contrôle et l'opérateur de l'application.

La solution s'oriente donc plutôt vers un calcul de l'empreinte après chiffrement. Or, dans ce cas, l'intégrité concerne le fichier chiffré, et non le document d'archive lui-même. Cela induit un risque juridique car l'ensemble de la chaîne de preuve confère à un document qui n'est pas le document intelligible mais un objet non intelligible.

Par ailleurs, si le document doit être communiqué en tant que preuve à un magistrat ou à l'administration, celui-ci (ou celle-ci) aura besoin de l'archive non chiffrée pour la lire. La vérification d'intégrité par un magistrat (empreinte du document = empreinte journalisée) ne sera donc pas conforme. L'alternative serait de communiquer l'archive électronique chiffrée au magistrat et de lui donner une clé de déchiffrement. Ceci induit un risque juridique de non recevabilité de la preuve pour des raisons techniques ou culturelles des instances judiciaires, qui préfèreront très certainement un media plus traditionnel.

La solution la moins risquée consiste à conserver les deux empreintes : l'empreinte de l'archive non chiffrée, qui servira au moment de la communication (consultation, remise à un tiers, …) et qu'il conviendra de journaliser, et l'empreinte de l'archive chiffrée qui servira aux contrôles d'intégrité par le service d'archivage numérique ou le tiers archiveur, qui n'a pas le besoin d'en connaître. Cette empreinte devra également être journalisée.

7.4.2 - Indexation

Le chiffrement des archives numériques induit l'impossibilité (avec des solutions courantes) d'indexer les contenus d'archives par les indexeurs plein texte. Il n'est bien évidement pas préconisé d'indexer en plein texte avant le chiffrement, car tout ou partie du contenu du document serait alors conservé dans l'index du moteur de recherche en clair et rendrait caduque l'objectif de confidentialité renforcée.

Il est néanmoins nécessaire de pouvoir rechercher des archives selon des métadonnées appropriées, définies par l'archiviste et ne présentant pas de caractère confidentiel mais qui restent cependant suffisantes pour que l'utilisateur puisse retrouver une archive.

Si cet exercice n'est pas possible, l'utilisateur ne disposera pas d'instrument de recherche. Le SAE sera alors dans un usage de simple conservation sans valeur ajoutée archivistique.

Dans le cas de métadonnées documentaires associées au fichier d'archive (AIP, voir § 7.2 -), ce fichier de métadonnées ne devra pas être intégré dans l'enveloppe chiffré afin de permettre leur indexation par les moteurs de recherches ou l'import par les fonctions documentaires métier.

7.4.3 - Transchiffrement

Les spécifications des algorithmes de chiffrement ainsi que les longueurs de clés évoluent régulièrement. Les choix réalisés en 2015 au moment du versement du document d'archive pourraient être remis en cause dans l'avenir.

Cela induit de prendre un nouveau champ d'application dans les processus de conservation : la migration de chiffrement ou « transchiffrement ». Il s'agit de déchiffrer les archives et de les rechiffrer selon le nouvel algorithme et/ou la nouvelle longueur de clé. Ceci implique une connaissance du secret par l'opérateur ou par l'application de migration, car il n'est pas envisageable de demander à chaque utilisateur de transchiffrer les archives qu'il aurait versées des années auparavant.

Le procédé de transchiffrement devra garantir l'intégrité de l'archive en clair (le format de l'archive n'étant pas modifié, son empreinte non plus).

7.4.4 - Migrations de format du contenu d'une archive chiffrée

Le processus de migration du format d'une archive chiffrée pour un besoin de pérennité nécessite :

- de déchiffrer l'archive à migrer ;
- de réaliser l'opération de migration du format ;
- de calculer l'empreinte après migration ;
- de rechiffrer l'archive migrée ;
- de calculer l'empreinte après chiffrement.

7.4.5 - Déchiffrement permanent

Les opérations visant à déclassifier une archive nécessitent un déchiffrement avec conservation seule de l'empreinte de l'archive ainsi déchiffrée.

7.4.6 - Capacités du système

Selon les choix de longueur des clés et des algorithmes, il est important de bien qualifier les puissances de calcul nécessaires au système pour assurer les chiffrements lors des versements, des déchiffrements et des consultations, et d'adapter les engagements de performances en conséquence.

Il est également important de rester vigilant sur l'augmentation du nombre de clés et la capacité des systèmes à gérer durablement une volumétrie croissante, notamment si le niveau de granularité de chiffrement est fin (au document par exemple).

7.5 - Le chiffrement des secours

De la même manière que la conservation, le chiffrement des secours sur site de continuité ou reprise d'activité doivent suivre les mêmes logiques de chiffrement que celui du site nominal.

Concernant les sauvegardes sur supports amovibles, du fait que le contenu est chiffré, un surchiffrement du support n'apportera pas beaucoup de sécurité complémentaire. Cependant, le stockage des supports doit être réalisé dans un environnement sécurisé pour répondre au besoin de disponibilité en cas de crise ou de perte de données.

7.6 - Le chiffrement des Métadonnées

7.6.1 - Métadonnées en base

Le chiffrement des métadonnées contenues dans une base de données répond aux mêmes logiques expliquées précédemment. Il s'agit d'un domaine plus commun à l'ensemble des SI qui n'est pas développé dans ce Guide.

A la différence d'un SI métier, qui peut contenir des données confidentielles (santé, informations bancaires, …), les métadonnées documentaires d'un Système d'Archivage Électronique constituent un instrument de recherche. Il n'est pas toujours nécessaire d'intégrer les métadonnées confidentielles dans le système d'archivage. Si les données confidentielles sont nécessaires à la recherche, il conviendra de séparer l'affichage des champs contenant les données confidentielles de ceux contenant les données confidentielles, et de permettre l'accès aux données confidentielles aux seuls profils autorisés. Les champs confidentiels peuvent êtres chiffrés en cas de besoin de sécurité particulier.

7.6.2 - Métadonnées dans les fichiers associées à l'archive.

Les métadonnées documentaires peuvent êtres modifiables et évoluer en fonction des nouveaux besoins de consultation. Au même titre que les données en base, il conviendra de restreindre les informations confidentielles du fichier de métadonnées associé à l'archive, et de ne pas les chiffrer pour garder une souplesse dans l'indexation et la modification. S'il s'avère nécessaire d'intégrer des métadonnées confidentielles, un fichier de métadonnées confidentielles pourra être chiffré avec l'objet d'archives lui-même.

Il est à noter que le chiffrement des métadonnées induit la même problématique d'indexation par les moteurs de recherches et les possibilités de requête en base.

7.7 - Convention de chiffrement

Lorsque l'usage de technologies de chiffrement est employé par un opérateur tiers, il convient de définir une convention de chiffrement où sont formalisées les modalités suivantes :

- une définition des objectifs de sécurité ;
- une modélisation des mécanismes mis en œuvre ;
- une spécification du niveau de robustesse attendu ;
- le droit ou non-droit qu'a l'opérateur par rapport à l'usage et à la possession de clés ;
- les moyens et procédures de recouvrement en cas de perte de clés ;
- le format de réversibilité du fond chiffré ainsi que les clés permettant de déchiffrer ;
- la consigne pour l'opérateur en cas de saisie par une autorité judiciaire nationale ou internationale ;
- les niveaux de chiffrement des différentes métadonnées ;
- les procédures de migration et de transchiffrement ;
- etc.

8 - AUTRES OPTIONS POUR UN RENFORCEMENT DE LA CONFIDENTIALITÉ

8.1 - L'anonymisation

L'anonymisation peut intégrer différentes techniques, comme la suppression de métadonnées, le floutage ou l'injection d'informations fictives. Cela peut être réalisé sur l'objet conservé ou sur les copies pour consultation par exemple.

L'anonymisation d'une archive modifiera forcément son intégrité. L'usage d'archives anonymisées est particulièrement ciblé pour les besoins de recherches scientifiques, mais s'éloigne du concept d'archivage à vocation probatoire, puisque l'archive anonymisée a perdu son intégrité et ne constitue plus un original ou une copie fidèle.

8.2 - Différencier le besoin de consultation du besoin de conservation

Comme vu dans les paragraphes précédents, il est important de bien différencier les besoins. Le numérique permet avant tout une meilleure accessibilité au document : il répond au besoin de consultation. L'archivage, quant à lui, répond, entre autres, au besoin d'intégrité lorsque l'archive possède une valeur juridique.

Le choix de répondre à ces deux besoins avec une même solution numérique induit une imbrication des technologies de gestion de l'intégrité/pérennité à celles de la confidentialité, notamment quand le chiffrement de la conservation est envisagé. Ce choix nécessite la mise en œuvre de l'ensemble des concepts, parfois contraignants, précédemment exposés.

Une alternative consiste à dupliquer les fonds selon leurs usages.

Fonds « en ligne ». Un premier fonds dit « en ligne », accessible et exposé, répond au besoin de consultation sans intégrer les fonctions de gestion d'intégrité. Il peut intégrer les technologies de chiffrement. Il s'agira d'un fonds de « copie d'archives » qui peut avoir des durées de mise à disposition selon sa valeur d'usage : dès que les taux de consultation deviennent très faibles et ne justifient plus les coûts de ce niveau de service, il peut être supprimé.

Fonds « hors ligne ». Un second fonds dit « hors ligne », peu exposé, répond au besoin d'intégrité et de gestion de la pérennité. Ce fonds n'est pas chiffré. Il s'agit du fonds d'archives des originaux répondant aux durées de conservation réglementaires. Pour les documents nativement physiques, il s'agira par exemple de conserver les fonds physiques après numérisation, pour un coût faible puisque le besoin de consultation sera porté par le fonds « en ligne ».

Cette alternative induit un double investissement qui doit être comparé, en termes de coût et de risques, à une solution unique gérant à la fois l'intégrité et le chiffrement.

9 - TIERS ARCHIVEURS / CLOUD / SOLUTION INTERNE

Le choix du positionnement du service d'archivage est important dans la stratégie de confidentialité. Il s'agit de choisir le niveau d'exposition au risque par rapport à l'extérieur et l'intérieur de la solution envisagée.

9.1 - Tiers archiveurs numériques

La raison d'être d'un tiers archiveur est de faire bénéficier au client d'un effet de mutualisation des investissements et des ressources d'exploitation principalement sur la sécurité. Le métier du tiers archiveur est de mettre en œuvre les moyens pour la sécurité d'une solution d'archivage et uniquement pour l'archivage.

Par opposition, l'archivage est rarement la première priorité d'une DSI qui concentre généralement ses efforts en termes de confidentialité sur ses SI[60] métiers.
L'externalisation des fonds numériques chez un tiers archiveur est un moyen simple de segmentation des rôles ; il s'agit d'un principe de base en termes de confidentialité. En effet, une infrastructure d'archivage exploité par un tiers archiveur permet de séparer les rôles avec l'exploitation d'une DSI interne, car cette dernière n'aura aucun accès technique aux environnements de conservation.

9.2 - Solution interne

L'avantage d'une solution interne est qu'elle permet une meilleure prise en charge des accès utilisateurs, notamment si l'entreprise a mis en place des solutions de fédération des identités et des accès.

Une solution interne sera également moins exposée si elle reste très fermée dans l'environnement de l'entreprise. S'il s'agit au contraire d'ouvrir le système vers l'extérieur (extranet, nomadisme,…), les problématiques de gestion des accès et d'authentification de l'utilisateur seront à gérer au même titre qu'une solution externalisée.

9.3 - Cloud

Le Cloud, au sens « externalisation de la conservation et des applications » peut sembler une solution économique. Il existe de nombreuses configurations d'externalisation de cloud qui vont de la simple location d'espace à l'exploitation et l'administration avancée des systèmes.
Selon l'architecture choisie et le niveau de maîtrise sur ces types d'infrastructures, le degré d'exposition variera considérablement, ainsi que le niveau de complexité des solutions d'archivage pour assurer la confidentialité et la pérennité. In fine, une solution interne ou Tiers Archiveur peut s'avérer plus économique et moins risquée.

60. Système d'Informations

10 - RÉFÉRENTIELS ET CERTIFICATIONS

Les certifications NF 461 (conformité à la norme AFNOR NF Z42-013), NF Logiciel Composant coffre-fort numérique (conformité à la norme AFNOR NF Z42-020), ISO 27001 (SSI), les Labels FNTC TA, FNTC CFN, CNIL services de coffre-fort numérique, les certifications CSPN et RGS de l'ANSSI, ainsi que les agréments du SIAF et ASIP Santé sont autant de moyens pour assurer la conformité et la confiance. Le recours à des tiers archiveurs ou des éditeurs certifiés, l'achat de solutions informatiques fonctionnellement compatibles, ainsi que la mise en œuvre de ces référentiels par les donneurs d'ordres eux-mêmes apportent la confiance nécessaire à la mise en œuvre et la protection de la confidentialité.

Cf Guide Normes et labels de la dématérialisation :
https://www.fntc.org/fr/publications/func-startdown/375/

11 - CONCLUSION

La confidentialité de l'information a toujours été un sujet sensible et paradoxal : bien des citoyens demandent de la transparence pour les autres, revendiquent le respect de la vie privée pour eux-mêmes tout en diffusant leurs photos personnelles sur les réseaux sociaux. Les états renforcent les exigences de confidentialité, mais se réservent, pour certains, un « droit » d'accès aux informations (confidentielles ou pas), avec la motivation de protéger des intérêts vitaux. Il s'agit de paradoxes qui reflètent la réalité d'une démocratie bien vivante : **tant que nous pouvons débattre de la confidentialité et de la transparence, la démocratie se porte bien !**

Les archives sont également un fondement de la démocratie. Elles « posent » l'histoire, constituent des « preuves » démontrant l'application du droit. Les archives contribuent à l'Etat de droit, ne serait-ce que par leur existence et leur intégrité.

Afin de préserver la confidentialité des archives, et préalablement à toute conception de solution, il est nécessaire de bien cerner le cadre réglementaire des archives, ainsi que les risques liés à une divulgation des informations qu'elles contiennent. Une classification documentaire est indispensable au démarrage d'une réflexion sur la confidentialité. **Les solutions dépendront du niveau de protection requis par chaque niveau de classification.**

Les vols de données font néanmoins de plus en plus la une des médias, et contribuent à un sentiment d'insécurité, voire de défiance, envers le traitement des données numériques. Pour se rassurer, la société cherche des solutions : certains réglementent, d'autres proposent des technologies de sécurité. Ceci présente **le risque de créer des systèmes juridico-techniques complexes** qui pourraient produire un effet inverse avec le contournement desdits systèmes par les utilisateurs.

Au-delà de la garantie d'intégrité, un renforcement des exigences de sécurité peut être bénéfique, mais il faut garder à l'esprit qu'**un niveau de confidentialité très élevé aura un impact sur la disponibilité de l'information** et son usage par l'utilisateur final. Une bonne pratique consiste à fixer ses objectifs pr**écis** pour chacun des critères de disponibilité, d'intégrité et de confidentialité dans un projet d'archivage.

La solution du chiffrement est séduisante. Ce guide montre qu'elle peut être pertinente pour répondre à un niveau de confidentialité élevé, dans une organisation parfaitement maîtrisée et avec des ressources financières proportionnelles au niveau d'exigence. Néanmoins, que la solution d'archivage chiffre ou ne chiffre pas, il sera toujours nécessaire de faire confiance à certains acteurs opérant la solution : l'utilisateur, l'administrateur, l'exploitant interne, le fabricant de solutions de sécurité, etc.

La confiance est donc nécessaire mais il ne s'agit pas d'accorder une confiance « aveugle ». Elle doit se gagner par l'opérationnalité de fonctions de sécurité et la robustesse des organisations. Cela nécessite un audit du système d'archivage sur la base de référentiels ou de normes. Les autorités d'agrément, les organismes de certification et labélisation sont autant d'acteurs efficaces sur qui se reposer pour attester du respect des bonnes pratiques.

Les tiers de confiance se donnent pour mission d'offrir des fonctionnalités documentaires innovantes tout en préservant la confidentialité des archives. A ce titre, ils **sont un atout pour la transition numérique** notamment pour aider le marché à définir le meilleurs compromis sécurité / usage / coût des archives.

12 - REMERCIEMENTS

Comité de rédaction :

Pascal Agosti	SELARL CAPRIOLI & Associés, Société d'Avocats
Pierre-Jean Aubourg	Bull, an Atos Company
Arnaud Belleil	Cecurity.com
Alain Bobant	Huissier de justice, Président FNTC
Alain Borghesi	Cecurity.com
Denis Bourdillon	Asterion France
Isabelle Cantero	SELARL CAPRIOLI & Associés, Société d'Avocats
Eric Caprioli	SELARL CAPRIOLI & Associés, Société d'Avocats
Marc Chédru	Marc Chédru Conseil
Bruno Couderc	Bruno Couderc Conseil
Antoine Laurent	Docapost DPS
Hervé Streiff	Locarchives
Rui Teixeira Guerra	Darwin

Groupe Archivage de la FNTC

Acoss ; Alphacode ; Argus DMS ; Asterion ; Bruno Couderc Conseil ; Bull ; Cecurity.com ; CertEurope ; CNHJ ; Coffreo ; Conex ; Corus ; CS-OEC ; Darwin ; Data One ; DataSyscom ; Docapost ; edocGroup ; Esker ; G.L.I. Services ; Gdoc Lasercom ; Imprimerie Nationale ; Locarchives ; Marc Chédru Conseil ; Novarchive ; Opus Conseils ; Perfect Memory ; Primobox ; SELARL Caprioli & Associés, société d'avocats ; Tessi Ged ; Worldline ; YouSign.

A propos de la FNTC

La Fédération des Tiers de Confiance (FNTC) regroupe un ensemble de professionnels fournisseurs et/ou utilisateurs de services numériques : institutions, entreprises de taille variée, start-ups et experts techniques et juridiques.
Créée en 2001 par un ensemble d'acteurs institutionnels et de prestataires de services suite à la loi du 13 mars 2000, afin de structurer les échanges numériques naissants, la FNTC a désormais pour vocation à étendre son action au niveau international avec l'ensemble des acteurs qui souhaitent développer la confiance dans le numérique, que ce soit en Europe, dans les pays Francophones ou ailleurs.
Son action s'articule autour de trois missions :

- Promouvoir les techniques et méthodes pour garantir la confiance dans le numérique et favoriser la connaissance des meilleures pratiques.
- Construire la confiance dans le numérique de demain.
- Accompagner les institutions publiques.

Les adhérents et membres associés FNTC

Accelya ; ACN ; ACOSS ; Actradis.fr ; AFCDP ; Agro Edi Europe ; Alain Ducass ; AllPerf ; Almerys ; Alphacode ; André Giudicelli (Université de la Rochelle) ; Argus DMS ; AriadNext ; Arturo Galindo Baquero (Colombie) ; Association Apeca ; Asterion ; Axemio ; Bernard Starck ; Bruno Couderc Conseil ; Bull ; Caprioli & Associés ; Cecurity.com ; Celtipharm ; CertEurope ; ChamberSign ; Chambre des Huissiers de Justice du Québec ; Chambre Nationale des Huissiers de Justice ; Cleona ; CNHJC (Cameroun) ; Coffreo ; Compagnie Nationale des Commissaires aux Comptes ; Conex ; Conseil National des Greffiers des Tribunaux de Commerce ; Conseil Supérieur de l'Ordre des Experts-Comptables ; Corus ; Cryptolog ; CV Trust ; Cyril Murie ; Darva ; Darwin Consulting & Finance ; Data One ; Data Syscom ; Demaeter ; Dhatim ; Dhimyotis ; Dip Africa (Côte d'Ivoire) ; Docapost BPO ; Docapost DPS ; Document Channel ; DPII-Telecom ; Ecosix ; Edificas ; Edilink ; Edokial ; EdocGroup ; Eestel ; Elcimai Financial Software ; Election-Europe ; ESI ; Esker ; Esopica ; Euro-Vote ; Fabrice Mattatia ; Forum Atena ; G.L.I Ingenierie et Services ; GDoc Lasercom ; Gérard Cathaly ; Guy de Felcourt ; Hénon Conseil ; Hervé Schauer Consultants; I-Invest ; Imprimerie Nationale ; In Continu et Services ; InTech (Luxembourg) ; Interb@t ; Isilis ; Issendis ; jedeclare.com ; Kahn & Associés ; L3i (Laboratoire Informatique, Image et Interaction) ; la Banque Postale ; Laboratoire Cyberjustice (Montréal – Québec) ; Laurent Voillot ; LegalBox ; LeMore Avocats ; Locarchives ; Maileva ; Marc Chédru Conseil ; Marie-Anne Chabin ; MGMR ; Mipih ; Multicert (Portugal) ; MyProcurement ; Napps (USA) ; Netheos ; Notarius (Canada); Novapost ; Novarchive ; Ocentis ; Odyssey Services ; OFSAD ; One Legal (USA) ; OpenTrust ; Opus Conseils ; Perfect Memory ; Philippe Amblard (maître de conférences Paris 8) ; PPI ; Primobox ; Provigis ; René Beauchard ; Sagemcom ; Scala ; Sealweb ; Sogelink ; Sood ; Stocomest ; Syrtals ; Tarvi Martens ; TeleTrust (Allemagne) ; Tessi GED ; Thierry Amadieu ; Transparency Rights ; Union Internationale des Huissiers de Justice et Officiers Judiciaires ; Univers Monétique ; Vialink ; Voxaly Electionneur ; Wacom ; We proov ; Worldline ; Xeonys ; Yousign

FNTC
Fédération des Tiers de Confiance
19 rue Cognacq-Jay
75007 Paris

conception graphique : www.idsg.fr