Université Toulouse Jean Jaurès

UFR d'histoire, arts et archéologie

Département documentation, archives, médiathèque et édition

Les systèmes d'archivage électronique à l'épreuve de la cybersécurité moderne

État de l'art, vulnérabilités et perspectives d'évolution pour une protection durable des archives numériques

Renée Elodie HOUNTOHOTEGBE

Volume 1 : texte et bibliographie

Mémoire présenté pour l'obtention du Master I Information-Documentation

Sous la direction de Mr. Taoufik DKAKI

Juin 2025

Département Documentation Archives, Médiathèque et Édition

UNIVERSITÉ TOULOUSE Jean Jaurès

Remerciements

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce mémoire.

Je remercie tout d'abord Mr. Taoufik DKAKI mon directeur de mémoire, pour son accompagnement, sa disponibilité et ses conseils éclairés dans le cadre de ce sujet. Sa bienveillance et ses exigences m'ont permis de progresser tant sur le plan méthodologique que réflexif.

Je tiens également à remercier les enseignants et intervenants du Master 1 Information - Documentation de l'Université Toulouse Jean Jaurès pour la richesse de leurs enseignements, ainsi que pour leur implication tout au long de cette formation.

Ma reconnaissance va aussi à l'équipe de Congo Digital Services (CDS) et à **Alessya Consulting**, pour m'avoir offert l'opportunité de mener une étude concrète dans un environnement professionnel stimulant. Je remercie plus particulièrement Fred Arly Kaya, pour sa confiance, ainsi que mes collègues pour leur collaboration et leur esprit d'équipe, notamment lors de l'élaboration du projet de système d'archivage électronique.

Enfin, je n'oublie pas ma famille et mes proches, dont le soutien moral, la patience et les encouragements constants ont été essentiels à chaque étape de ce travail.

À toutes et à tous, **merci**.

Sommaire

Remerciements 3
Introduction Générale 6
PARTIE I 8
Cadre théorique : entre archivage numérique et cybersécurité 8
Chapitre 1 - Fondements et normalisation des systèmes d'archivage électronique 10
1.1 Définition et finalités d'un Système d'Archivage Électronique (SAE) 10
1.2 SAE vs coffre-fort électronique : distinctions et complémentarités 12
1.3 Le rôle des prestataires de confiance et la notion de SAE qualifié 14
1.4 Typologie des objets numériques à archiver et des enjeux autours 16
1.5 Normes et référentiels essentiels 18
Chapitre 2 - La sécurité dans les systèmes d'information et les SAE 20
2.1 Les grands principes de la sécurité informatique : fondements de la résilience documentaire dans les SAE 20
2.2 Architecture sécurisée d'un SAE 23
2.3 Cas particuliers : signature électronique, horodatage, empreinte numérique 25
2.4 Réglementation et gouvernance de la sécurité 27
Chapitre 3 - Menaces émergentes et vulnérabilités des SAE 30
3.1 Cartographie des cybermenaces 31
3.2 Études de cas de cyberattaques récentes touchant des administrations 34
3.3 Vulnérabilités liées à l'obsolescence technologique et à la pérennité des formats... 36
3.4 L'intelligence artificielle : risque émergent ou levier défensif pour les SAE ?..... 37
PARTIE II 41
Analyse critique et perspectives : vers une cybersécurisation durable des SAE 41
Chapitre 4 - Évaluation des capacités actuelles de défense des SAE 43
4.1 Présentation de Congo Digital Service, filiale congolaise de l'entreprise Alessya Consulting 43
4.2 Analyse critique des dispositifs existants 45
4.3 Analyse des politiques de sauvegarde, de redondance et de récupération après sinistre 46
4.4 Problèmes d'interopérabilité et de continuité d'exploitation 48
4.5 Lacunes en matière d'agilité et d'adaptation face aux menaces dynamiques..... 50

Chapitre 5 - Innovations et solutions émergentes pour renforcer la cybersécurité des SAE 52
5.1 Blockchain et archivage à valeur probatoire..... 52
5.2 Wallets numériques : une piste prometteuse pour la gestion d'identité et le partage sécurisé dans les SAE 54
5.3 Intelligence artificielle et cybersécurité prédictive : un déséquilibre entre acteurs défensifs et pirates 56
5.4 Standards européens et certification de confiance : une excellence à étendre, mais à rééquilibrer..... 57
Chapitre 6 - Recommandations pour une stratégie de résilience des SAE..... 59
6.1 Intégration des principes de cybersécurité dès la conception du SAE 59
6.2 Renforcement des audits de sécurité et de la gestion des vulnérabilités 61
6.3 Sensibilisation, formation et culture de la sécurité pour les archivistes 62
6.4 Vers un modèle de gouvernance adaptative et collaborative..... 64
Conclusion générale 67
Bibliographie 69
Table des matières 74

ANNEXES (volume 2)

Introduction Générale

Sous l'effet conjugué de la dématérialisation des procédures administratives, de la généralisation des systèmes d'information et de l'émergence de nouveaux usages collaboratifs, les volumes de données numériques ont augmenté de manière exponentielle. Cette expansion, qualifiée parfois de "déluge numérique", s'accompagne **d'enjeux majeurs en matière de préservation de la mémoire** (l'information**),** notamment en archivage numérique**.** L'archivage traditionnel est devenu un « mode de conservation et d'organisation des archives sous une forme et dans une disposition qui permettent leur exploitation directe par des outils informatiques » [1]. La transformation numérique des organisations a donc profondément renouvelé les modalités de production, de gestion et de conservation des documents.

Dans ce contexte, des solutions de Gestion électronique des documents (GED) et de systèmes d'archivage électronique (SAE) sont devenus des dispositifs essentiels pour la structure et la gestion de la préservation des documents (archives) numériques. Conçu pour garantir, sur le long terme, l'intégrité ; l'authenticité ; la pérennité et l'accessibilité de l'information documentaire, leur vocation primaire repose sur la **sécurité de l'information**. En effet, les mesures de sécurité mises en place dans ces outils visent à protéger les documents contre tout accès non autorisé, les modifications, les suppressions ou les falsifications. Cela garantit la disponibilité de l'information documentaire et prévient de tout préjudice lié à sa divulgation ou altération.

Cependant, avec la montée en puissance des cybermenaces comme les attaques par rançongiciels, les intrusions ciblées, les exploitations de failles logicielles ou encore la manipulation de données ; l'ensemble des infrastructures numériques est soumis à un défi constant de sécurité.

Les archives sont indispensables pour assurer la continuité juridique, administrative et patrimoniale des organisations. La protection durable des archives dans un environnement numérique, au-delà de leur stockage, exige une réflexion poussée sur les capacités sécuritaires des SAE en tant que logiciel informatique. Ceci, afin d'appréhender leurs limites et les perspectives d'amélioration en cette ère de cybersécurité avancée.

C'est dans cette perspective que s'inscrit le présent mémoire. Il vise à analyser dans quelle mesure les systèmes d'archivage électronique actuels disposent des capacités techniques et

normatives nécessaires pour résister aux cybermenaces contemporaines et émergentes**,** tout en assurant la pérennité, l'accessibilité et la sécurité des documents conservés. La problématique de ce sujet peut ainsi être formulée de la manière suivante : **Les systèmes d'archivage électronique disposent-ils des capacités techniques et évolutives nécessaires pour assurer une protection durable des archives face aux cybermenaces actuelles et émergentes ?**

Pour y répondre, nous avons adopté une méthodologie qualitative, reposant sur une revue théorique approfondie des normes, référentiels et publications spécialisées dans les domaines de l'archivage électronique et de la cybersécurité. Cette revue est ensuite complétée, dans la seconde partie de la rédaction, par une analyse critique des vulnérabilités observées dans les SAE. Appuyée par un entretien avec des informaticiens ainsi que sur une veille technologique ciblée concernant les innovations en matière de sécurisation de l'information, nous présenterons dans les prochaines lignes, une réflexion organisée autour de six axes complémentaires regroupés en deux grandes parties.

La Première partie dresse le cadre théorique de l'archivage électronique et de ses exigences de sécurité, en explorant successivement la normalisation des SAE, les fondements de la cybersécurité documentaire, et les principales menaces émergentes.
La Deuxième partie propose une analyse critique des dispositifs actuels de protection des SAE, en mettant brièvement en lumière leurs limites face aux risques de cybersécurité existants. Cette dernière partie ouvre également une perspective**,** où nous formulons des recommandations concrètes et analysons dans quelle mesure les solutions innovantes (blockchain, intelligence artificielle, Wallet) pourraient constituer une stratégie de résilience durable des systèmes d'archivage électronique.

PARTIE I

Cadre théorique : entre archivage numérique et cybersécurité

Les archives sont définies par le code du patrimoine comme étant « l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité »[2]. Dans le contexte actuel du numérique, le terme ‘’ données ‘’ renvoie à une diversité d'objets numériques. Autrefois assimilé en archivage, aux documents numériques ou de substitutions (numérisés), l'archivage de la donnée prend aujourd'hui une tout autre ampleur.

Au-delà des documents numériques tels que les fichiers texte, les feuilles de calcul ; les documents audiovisuels, les bases de données ; les images ; e-mails ; les sites web ; et même les messages sur les réseaux sociaux sont également considérés comme documents d'archives. Globalement, tout ce qui a une valeur d'information et qui peut témoigner de l'activité d'une personne ou d'une organisation est potentiellement archivable. Le système d'archivage électronique est une application dédiée à cette tâche. L'encadrement qu'offre cette solution informatique permet d'assurer le stockage pérenne de ces informations dans des conditions qui préservent leur intégrité et leur disponibilité à long terme.

Cependant, à l'instar de tout logiciel informatique, les SAE sont confrontées aux menaces cybernétiques. Compte tenu de la densité et de la sensibilité des informations gérées par ces derniers, des règles et standards normatifs ont été mis place pour assurer la sécurité de l'outil et de son contenu. Ce sont des normes qui ont été établit dans l'optique de créer une architecture sécuritaire adaptée à l'usage de l'outil.

Cette première partie de notre étude est structurée en trois chapitres. A partir de l'explication du fondement conceptuel, normatif et sécuritaire du système d'archivage électronique, nous analyserons les référentiels techniques et réglementaires qui encadrent leur mise en œuvre. Ensuite nous nous intéresserons aux cybermenaces actuelles afin de pouvoir identifier dans la seconde partie de ce mémoire, si nos SAE sont assez robustes ou facilement adaptatives face à ces menaces ou celles à venir.

Chapitre 1 - Fondements et normalisation des systèmes d'archivage électronique

Depuis l'apparition du numérique dans les pratiques archivistiques, des textes ont été élaborés en conséquence. Ce chapitre vise à clarifier les fondements conceptuels et fonctionnels du SAE : sa définition, ses objectifs, son articulation avec les prestataires de confiance, ainsi que les normes encadrant son déploiement. L'objectif de ce chapitre est d'appréhender les fondements actuels autour de l'usage de l'outil d'archivage électronique.

1.1 Définition et finalités d'un Système d'Archivage Électronique (SAE)

Le système d'archivage électronique (SAE) s'impose comme un outil stratégique pour garantir la pérennité, la fiabilité et la sécurité des informations produites ou reçues par les organisations. Il ne s'agit plus seulement de stocker des fichiers, mais bien de mettre en œuvre une véritable politique de conservation durable et encadrée de l'information numérique. Ceci, dans un souci de conformité réglementaire, de protection des actifs informationnels et de préservation de la mémoire institutionnelle. Traduit littéralement, l'expression "système d'archivage électronique" devrait englober un ensemble des matériels et technologies informatiques ainsi que de processus dont la finalité serait l'archivage. Autrement dit, c'est une combinaison d'outils matériels et de méthodes, incluant le matériel informatique, les logiciels, les normes, et les procédures.

Toutefois, on attribue souvent l'expression "système d'archivage électronique" à un logiciel car ce logiciel est la pièce maîtresse qui gère l'ensemble du processus. Il coordonne le stockage, l'indexation, la recherche, et la récupération des documents, ainsi que la conformité aux normes de conservation. Même si ce terme englobe un ensemble plus large d'éléments, le logiciel est souvent mis en avant car il est l'interface principale que les utilisateurs voient et utilisent. C'est donc sur ce logiciel que nous portons actuellement notre étude.

Sur le plan fonctionnel, le SAE peut être défini comme un dispositif logiciel spécifiquement conçu pour prendre en charge l'ensemble du cycle de vie des documents électroniques à valeur probatoire ou patrimoniale, de leur versement à leur élimination ou à leur conservation définitive. À ce titre, il assure la réception, l'organisation, la conservation, l'accessibilité, la traçabilité, la sécurité et, enfin, la destruction ou la réversibilité des archives, selon des règles strictement définies. Comme l'indique l'École de bibliothéconomie et des sciences de l'information (EBSI), la finalité du SAE est de permettre une conservation à long terme tout en

protégeant les documents de toute altération ou suppression non autorisée, dans le respect de leur valeur légale et administrative [1].

De fait, en dehors de leur capacité de structuration de l'information, les SAE « peuvent être davantage orientés sécurisation des données/documents à valeur probatoire ou pérennisation à très long terme des données/documents » ; car ils intègrent en leur sein un coffre-fort numérique afin de sécuriser au mieux les documents (données). Le coffre-fort électronique est par définition une combinaison logiciel/matériel qui permet de préserver l'intégrité d'objets numériques dans le temps [3]. Mais il arrive que par abus de langage, d'aucuns peuvent assimiler le SAE à un « coffre-fort numérique avec un accès aux informations en lecture seule et dont les autorisations d'accès sont définies à l'avance » [4].

Il faut surtout retenir que le SAE ne se limite pas qu'à être un simple entrepôt numérique. Il constitue un environnement structurant, piloté par des politiques de conservation normalisées, et doté de fonctions avancées de gestion des métadonnées, de contrôle d'accès hiérarchisé, de journalisation des opérations et de gestion du cycle de vie archivistique. Il est appelé à interagir avec les autres composantes du système d'information (SI) de l'organisation. Dans le SI, le SAE constitue une extension spécialisée, axée sur les exigences de pérennité, de conformité et de sécurité.

En termes de technologies, les systèmes d'information englobent des applications métiers et les systèmes de gestion de l'information [1]. Dans cet environnement, le SAE se positionne comme la destination finale des processus, garantissant la conservation à long terme et l'accès ultérieur aux informations, une fois qu'elles ne sont plus actives (couramment demandées/utilisées) dans les systèmes d'informations. Le SAE avec ses spécificités archivistiques, doit donc être interopérable avec le SI pour une gestion fluide et efficace de l'information.

Sur le plan stratégique, les finalités d'un SAE sont multiples. D'une part, il s'agit d'assurer la conservation à long terme des documents en dépit des évolutions technologiques, en particulier des risques liés à l'obsolescence des formats, à la disparition des supports physiques, ou encore aux incompatibilités logicielles. Des dispositifs comme le modèle OAIS (Open Archival Information System), standardisé par la norme ISO 14721, offrent à cet égard une grille de lecture conceptuelle des fonctions que doit remplir tout système de préservation numérique : ingestion, stockage, gestion des données descriptives, accès, administration et planification de

la pérennité. Cette approche systémique vise à garantir que l'information archivistique reste exploitable et compréhensible dans le temps, même en cas de changement technologique profond [5].

D'autre part, la finalité du SAE réside également dans sa capacité à servir de socle de confiance pour l'archivage probatoire. En encadrant techniquement et juridiquement les processus de dépôt, de gestion et de restitution des documents numériques, il renforce la force juridique des archives conservées, en particulier dans le cadre de litiges, d'audits ou de contrôles. La mise en œuvre de mécanismes tels que l'empreinte numérique (hash), le sceau électronique, l'horodatage ou la signature numérique permet d'attester de l'intégrité originelle du document et de l'identité de son émetteur, à condition que ces éléments soient vérifiables a posteriori dans le SAE [1].

Enfin, nous devons distinguer clairement le SAE d'autres dispositifs apparentés, notamment le coffre-fort électronique (CFE). Ce dernier, bien qu'utilisé pour garantir l'intégrité et l'authenticité des documents, notamment à valeur de preuve, n'intègre pas l'ensemble des fonctions archivistiques couvertes par un SAE. Le SAE, contrairement au CFE, permet d'organiser le cycle de vie documentaire dans sa globalité, incluant la description archivistique, l'évaluation, l'accès contrôlé, la traçabilité et la réversibilité. Il peut néanmoins intégrer un module de coffre-fort électronique, agissant comme un composant parmi d'autres au sein de son architecture globale [1].

1.2 SAE vs coffre-fort électronique : distinctions et complémentarités

Dans l'écosystème de l'archivage numérique, la distinction entre **système d'archivage électronique (SAE)** et **coffre-fort électronique (CFE)** demeure souvent floue, tant dans les discours professionnels que dans les pratiques institutionnelles. Pourtant, ces deux dispositifs répondent à des logiques différenciées tant sur le plan fonctionnel que normatif. Bien qu'ils puissent coexister au sein d'une architecture documentaire, les confondre reviendrait à méconnaître les spécificités techniques et juridiques qui les caractérisent, ainsi que les usages distincts auxquels ils sont destinés.

Le **SAE** se définit comme une **infrastructure documentaire complète**, conçue pour assurer l'ensemble du cycle de vie des archives électroniques. Il prend en charge les processus de **réception, d'identification, de classement, de conservation, de consultation, de traçabilité,**

et le cas échéant, de destruction des documents. Il intègre des logiques archivistiques formalisées, reposant sur des référentiels comme le modèle OAIS ou la norme NF Z42-013 et s'inscrit dans une temporalité souvent longue voire illimitée. Par sa nature, le SAE doit pouvoir **accueillir des volumes importants de documents**, de formats variés, et répondre à des obligations juridiques et organisationnelles issues notamment du **Code du patrimoine**, lequel encadre les règles de conservation, de communicabilité et de transfert des archives publiques.

Le **coffre-fort électronique (CFE)**, en revanche, est un **composant technique spécialisé**, généralement intégré dans un système d'information ou mobilisé en complément d'un SAE. C'est un espace de stockage numérique sécurisé conçu pour conserver des documents électroniques de manière pérenne et inviolable [6]. Contrairement à un simple stockage cloud (dont le niveau de sécurité peut varier en fonction du fournisseur), le coffre-fort électronique offre des mécanismes de protection avancés, comme la signature électronique, l'horodatage et des systèmes de cryptage garantissant que les documents ne peuvent pas être altérés [7]. C'est donc l'ensemble des mesures de protection mise en place pour garantir l'intégrité des documents qui permet de donner le caractère de coffre-fort numérique au dispositif de stockage.

La norme **NF Z42-020** sert de socle pour définir les exigences en matière de sécurité et de pérennité des documents stockés dans des coffres-forts numériques. Elle présente globalement les exigences auxquelles doivent se soumettre les prestataires de CFE [5]. La **certification ISO 27001** intervient ensuite pour vérifier que le fournisseur dispose d'un système fiable de management de la sécurité des informations et protège chaque utilisateur contre la perte, le vol, l'altération, l'intrusion sur les données archivées [8], **[9]**. Ces textes s'imposent notamment dans les secteurs réglementés, où la garantie de conformité et la robustesse juridique des documents archivés sont critiques.

Loin d'être concurrents, ces deux systèmes peuvent être **articulés de manière complémentaire**. Le SAE, peut piloter un module de coffre-fort électronique pour assurer la conservation probatoire de certains documents sensibles, tout en gérant de façon standardisée des archives à faible enjeu juridique. Le SAE est donc davantage conçu comme une **solution systémique**, intégrée dans la stratégie globale de gouvernance de l'information, tandis que le CFE constitue une **brique technique** spécialisée, pouvant être activée en fonction des besoins en sécurité renforcée. Cette articulation permet aux organisations d'adopter une **stratégie**

d'archivage à plusieurs niveaux, modulable selon la criticité, la durée de conservation et les obligations légales associées à chaque catégorie documentaire.

En définitive, le **SAE** et le **coffre-fort électronique** relèvent de logiques techniques et fonctionnelles distinctes, mais non exclusives. Le premier constitue une solution intégrée, complète et archivistique, tandis que le second représente un outil de sécurisation juridique renforcée, focalisé sur la preuve de l'inaltérabilité. Leur complémentarité, lorsqu'elle est bien pensée, constitue un atout stratégique pour la mise en place d'une politique d'archivage numérique conforme, efficiente et résiliente face aux menaces cyber contemporaines.

1.3 Le rôle des prestataires de confiance et la notion de SAE qualifié

La sécurité juridique et technique des systèmes d'archivage électronique (SAE) ne dépend pas uniquement de leur conformité aux normes de conservation ou des dispositifs technologiques mis en œuvre. Elle repose également sur l'intervention d'acteurs habilités, appelés **prestataires de services de confiance**, qui agissent en tant que garants institutionnels de l'intégrité, de l'authenticité et de la traçabilité des documents numériques. Ces entités jouent un rôle pivot dans l'architecture de l'archivage à valeur probatoire, en fournissant des garanties de confiance indispensables dans les environnements réglementés et sensibles.

La législation européenne récente, notamment le **règlement (UE) 2024/1183 du 11 avril 2024**, introduit une définition précise du **service d'archivage électronique qualifié**. Selon ce texte, un tel service assure la réception, le stockage, la récupération et la suppression de données électroniques dans des conditions qui en garantissent la **durabilité, l'intégrité, la lisibilité, la confidentialité et la preuve de l'origine** pendant toute la période de conservation. Cette définition va au-delà des simples capacités techniques. Elle intègre des exigences de preuve juridique et de traçabilité continue, en exigeant que les documents archivés puissent faire l'objet d'une vérification automatique de leur intégrité à tout moment, de leur entrée jusqu'à leur extraction.

Le règlement précise également que seuls les **prestataires de services de confiance qualifiés**, c'est-à-dire reconnus comme tels par une **autorité nationale compétente** ou un **organisme de certification accrédité**, sont autorisés à délivrer ces services à valeur juridique renforcée [10]. Cette **qualification formelle** repose sur des audits réguliers, des critères de conformité rigoureux et une surveillance réglementaire active. Elle confère aux services rendus une

présomption légale de fiabilité, notamment dans le cadre de contentieux, d'audits ou de contrôles administratifs.

Nous devons donc noter une distinction essentielle entre un **SAE ordinaire** et un **SAE qualifié**. Un SAE interne peut parfaitement satisfaire aux exigences de conservation et de gestion documentaire ; cependant, en l'absence d'une certification de confiance, il ne bénéficie pas de la même force probante qu'un SAE qualifié. Cette dernière offre des garanties supplémentaires en matière de sécurité, de transparence et de traçabilité**,** validées par des procédures tierces indépendantes [11]. La confiance dans le système ne repose donc plus exclusivement sur les moyens techniques, mais sur un cadre institutionnel vérifié et une responsabilité juridique encadrée.

Les missions des prestataires de services de confiance dépassent largement la simple fourniture d'un espace de stockage sécurisé. Ces entités assurent également la **mise en œuvre de mécanismes cryptographiques avancés**, notamment :

- **Horodatage qualifié**, garantissant une datation fiable et certifiée des documents ;
- **Calcul d'empreintes numériques (hash)**, permettant la détection de toute modification;
- **Chaînes de traçabilité scellées**, assurant une journalisation inviolable des actions ;
- **Gestion sécurisée des identités électroniques**, fondée sur des certificats numériques et des politiques d'accès rigoureuses.

Ces dispositifs s'appuient sur des normes éprouvées, telles que la **NF Z42-013**, qui encadre les conditions d'archivage probatoire, ou la **NF Z42-020**, qui définit les exigences applicables aux **coffres-forts numériques**, souvent intégrés comme composants d'un SAE qualifié.

Le recours à ces prestataires est particulièrement justifié dans les secteurs fortement régulés comme : les administrations publiques, la santé, les finances, le secteur juridique ou les assurances. Dans ces contextes, les exigences en matière de **compliance**, de **conservation des preuves**, et de **confidentialité** atteignent un niveau élevé, que seules des infrastructures auditées, qualifiées et supervisées sont en mesure de satisfaire. Confier tout ou partie du processus d'archivage à un prestataire qualifié permet ainsi aux organisations de **mutualiser les responsabilités**, de **réduire les risques juridiques**, et de se conformer aux standards européens de cybersécurité et de confiance numérique.

En définitive, l'archivage électronique qualifié ne repose pas seulement sur des pratiques rigoureuses ou des logiciels performants. Il exige la certification par un **prestataire de services de confiance qualifié**, reconnu conformément aux réglementations en vigueur. Cette certification permet d'établir une **présomption légale** de l'intégrité et de l'authenticité des documents archivés. Autrement dit, même si un archiviste suit toutes les bonnes pratiques et utilise des outils de sécurité avancés, sans cette certification officielle, son système d'archivage ne bénéficie pas du statut **"qualifié"** au sens du règlement européen ; Ce qui fait des prestataires de confiance certifiés des **acteurs incontournables d'une gouvernance numérique sécurisée**, à la croisée des exigences archivistiques, juridiques et techniques. Le prestataire numérique semble être désigné aujourd'hui comme les principales entités habilitées à maintenir un haut niveau de sécurité dans les coffres forts numériques.

1.4 Typologie des objets numériques à archiver et des enjeux autours

L'efficacité d'un système d'archivage électronique (SAE) repose en grande partie sur une connaissance précise et contextualisée des documents et objets numériques qu'il est amené à prendre en charge. La typologie des objets numériques à archiver constitue une base stratégique pour définir les formats, la sécurité et les modalités d'accès. Elle oriente également les choix en matière de formats, de métadonnées, de mesures de sécurité et de modalités d'accès aux contenus.

Les documents archivés ne se limitent plus à des fichiers textuels statiques depuis plusieurs années. Le périmètre du patrimoine informationnel s'est considérablement élargi. Aux côtés des fichiers bureautiques classiques (textes, feuilles de calcul, présentations), le SAE doit désormais gérer des documents enrichis, des images numériques (fixes ou animées), des enregistrements sonores, des courriers électroniques avec leurs pièces jointes, des bases de données relationnelles ou documentaires, des extraits de sites web, des publications issues des réseaux sociaux, ainsi que des contenus produits par des logiciels métiers spécifiques. Cette diversité de formats reflète la transformation des modes de production de l'information, mais elle complexifie également les mécanismes de préservation.

Certains objets numériques présentent des particularités techniques qui exigent une vigilance accrue en matière de conservation. Les documents électroniques signés ou horodatés, les fichiers chiffrés ou encapsulant des métadonnées dynamiques sont autant d'exemples qui posent des défis spécifiques en termes d'authenticité, d'intégrité et de preuve [12]. Leur

conservation suppose non seulement la préservation du contenu binaire, mais aussi celle de la structure logique, du contexte de production, et des éléments de traçabilité associés. En l'absence d'une conservation rigoureuse de ces éléments constitutifs, la valeur probatoire du document peut être compromise.

La distinction entre documents « nativement numériques » et documents numérisés est également fondamentale. Les premiers, créés dès l'origine sous forme électronique, soulèvent des problématiques d'interopérabilité liées à l'environnement logiciel d'origine, dont la disparition peut rendre l'exploitation des contenus difficile. Les seconds, issus de processus de dématérialisation de documents papier, nécessitent une chaîne de numérisation traçable et contrôlée, appuyée par des dispositifs permettant de garantir l'équivalence fonctionnelle et juridique avec l'original physique [13]. Dans les deux cas, la gestion de la lisibilité et de l'exploitabilité dans le temps suppose des stratégies de migration, de normalisation ou d'émulation adaptées.

Chaque typologie implique des traitements différents, tant en termes de durée de conservation que de niveaux de sécurité requis. Les documents juridiques doivent bénéficier par exemple de mesures renforcées en matière d'intégrité et de traçabilité, tandis que les documents patrimoniaux nécessitent une attention particulière à la lisibilité future et à la contextualisation archivistique.

Par ailleurs, la question de la granularité des objets à archiver constitue un enjeu souvent sous-estimé. Un SAE doit être capable de gérer des documents isolés aussi bien que des ensembles documentaires complexes ou chaînés. Par exemple, un dossier administratif peut regrouper des dizaines de pièces de nature hétérogène, mais liées par une logique procédurale ou fonctionnelle. La cohérence de ces ensembles documentaires repose sur la capacité du SAE à structurer et à maintenir les liens entre les pièces, à travers un schéma de métadonnées explicite et conforme à un standard d'échange comme le **SEDA** (Standard d'échange de données pour l'archivage).

En somme, la diversité des objets numériques à archiver appelle à une approche souple, modulaire et évolutive. Le SAE ne peut fonctionner selon une logique figée : il doit intégrer des mécanismes d'adaptation aux nouveaux formats, aux nouvelles exigences de preuve, ainsi qu'aux pratiques émergentes de production documentaire.

1.5 Normes et référentiels essentiels

Le développement et l'exploitation efficiente d'un système d'archivage électronique (SAE) reposent sur l'adhésion à un cadre normatif structuré et rigoureux. Ce dernier constitue l'ossature conceptuelle et technique qui permet de garantir, dans la durée, la conservation fiable et sécurisée des documents numériques. L'archivage électronique ne peut être considéré comme maîtrisé que s'il s'appuie sur des normes reconnues, assurant la pérennité, l'intégrité, l'authenticité, l'interopérabilité et la valeur légale des objets archivés.

Parmi les normes structurantes, le **modèle OAIS** (Open Archival Information System)**,** établi par la norme **ISO 14721**, occupe une place fondatrice. Conçu à l'origine par le Consultative Committee for Space Data Systems **(**CCSDS**)** pour répondre aux besoins de l'archivage scientifique spatial, ce modèle a été généralisé à l'ensemble des systèmes d'archivage numérique. Il propose une architecture conceptuelle décomposée en six fonctions fondamentales : l'ingestion (ingest), la gestion administrative (administration), le stockage sécurisé (archival storage), l'accès (access), la gestion des métadonnées (data management) et la planification de la pérennité (preservation planning). Ce cadre fonctionnel, couplé à une définition précise des rôles producteur, consommateur et gestionnaire du système, permet d'orchestrer de manière systémique les processus archivistiques numériques, indépendamment des technologies sous-jacentes.

À l'échelle internationale, une autre norme majeure est la **série ISO 16175**, plus connue sous le nom de **ICA-Req**, développée sous l'égide du **Conseil international des archives**. Contrairement à OAIS, qui définit une structure organisationnelle, ICA-Req établit les **exigences fonctionnelles minimales** auxquelles un SAE doit satisfaire pour gérer des documents numériques en environnement administratif. Elle met l'accent sur la capacité des systèmes à assurer la **création, la capture, la gestion et la conservation** des documents tout en respectant les principes de fiabilité, d'intégrité et de traçabilité. En cela, ICA-Req constitue un instrument normatif essentiel pour garantir la conformité juridique des processus documentaires numériques.

Au niveau européen, le référentiel **MoReq2010 (Modular Requirements for Records Systems)**, porté par le DLM Forum, se distingue par son approche modulaire et évolutive. Plutôt que de proposer un corpus figé, il invite les organisations à construire leur SAE en fonction de modules interopérables adaptés à leurs besoins. MoReq2010 met l'accent sur

plusieurs dimensions clés, dont la gestion avancée des métadonnées, l'auditabilité complète des actions, la sécurité d'accès et la capacité à intégrer des politiques de conservation différenciées. Cette approche flexible s'avère particulièrement adaptée aux environnements hétérogènes et à forte volumétrie documentaire.

En France, l'encadrement normatif du SAE s'est développé à travers un ensemble cohérent de textes techniques. La norme **NF Z42-013** constitue la référence centrale pour les **archives à valeur probatoire**. Elle définit un ensemble de spécifications relatives à la conservation, l'intégrité, la traçabilité et l'inaltérabilité des documents numériques. Parmi les obligations figurent l'utilisation de mécanismes d'horodatage, le calcul d'empreintes numériques, la journalisation horodatée des opérations, ainsi que la mise en œuvre de mesures de sécurité préventives. Le guide **GA Z42-019**, désormais obsolète, servait de complément opérationnel en précisant les modalités d'application de la norme.

Pour les infrastructures à visée sécuritaire renforcée, telles que les **coffres-forts électroniques**, la norme **NF Z42-020** établit des spécifications techniques spécifiques. Elle s'applique à toute solution destinée à assurer la **conservation sécurisée et vérifiable** d'informations numériques dans des conditions permettant de maintenir leur intégrité sur le long terme. Cette norme est particulièrement pertinente pour les prestataires certifiés ou désireux d'acquérir le statut de **service de confiance qualifié** dans le cadre réglementaire européen.

L'interopérabilité entre systèmes d'archivage et la fluidité des transferts documentaires sont quant à elles garanties par la norme française **SEDA (Standard d'Échange de Données pour l'Archivage)**. Ce standard repose sur une structuration XML permettant l'échange de paquets d'archives accompagnés de leurs métadonnées. Il vise à assurer une continuité archivistique entre les entités productrices, les services versants et les dépôts d'archives définitives. Par sa granularité et sa souplesse, SEDA est aujourd'hui un pivot de la chaîne archivistique publique française, mais tend aussi à s'imposer dans des environnements mixtes ou privés.

Enfin, le cadre juridique global dans lequel s'inscrit l'archivage électronique en France repose sur le **Code du patrimoine**. Ce texte législatif encadre les obligations de **conservation, d'accessibilité, de tri et de communicabilité** des archives publiques, tout en définissant les responsabilités des services d'archives et les conditions de transfert des documents. Il constitue le fondement normatif qui articule les normes techniques et les exigences légales applicables

aux SAE, qu'ils soient mis en œuvre dans des contextes publics ou délégataires de service public.

En résumé, les normes et référentiels dédiés à l'archivage électronique ne représentent pas seulement un outil de conformité : ils forment un véritable **système de garantie** assurant la cohérence, la fiabilité et la durabilité des processus d'archivage numérique. Leur maîtrise conditionne la capacité des organisations à faire face aux risques d'altération, de perte, d'inaccessibilité ou de contestation des documents, tout en assurant la pleine valeur juridique et patrimoniale des archives conservées.

A travers ce premier chapitre, nous pouvons retenir que les SAE sont des logiciels de structuration d'information figée dans un format pérenne, conservés dans un environnement protégé dont il intègre les fonctionnalités sécuritaires. Ce résultat est obtenu grâce à l'encadrement des normes et standards intervenants dans l'archivage électronique et des solutions présentées par les prestataires des services de confiance, malgré la multiplicité et la diversité des données à gérer.

Chapitre 2 - La sécurité dans les systèmes d'information et les SAE

La sécurisation de l'information constitue un enjeu transversal dans l'ensemble des systèmes numériques. Conçus pour garantir la conservation pérenne des documents, les SAE doivent également intégrer des mécanismes de défense capables de prévenir les accès non autorisés, les altérations et les pertes d'intégrité. Dès lors, une question s'impose : comment les principes fondamentaux de la sécurité informatique sont-ils traduits dans l'architecture et le fonctionnement des SAE, et dans quelle mesure les cadres réglementaires actuels en assurent-ils l'effectivité ? Pour y répondre, ce chapitre examine successivement les grands principes de la sécurité de l'information, les dispositifs techniques sécurisant l'architecture d'un SAE, le cadre normatif applicable et les cas particuliers liés à l'authentification documentaire.

2.1 Les grands principes de la sécurité informatique : fondements de la résilience documentaire dans les SAE

La sécurisation des systèmes d'archivage électronique (SAE) repose sur une série de principes fondamentaux issus du champ plus large de la sécurité des systèmes d'information. Ces principes, au nombre de cinq, sont largement reconnus par les normes internationales et les

autorités de régulation, et s'avèrent incontournables pour garantir à la fois la **pérennité**, la **légalité** et la **fiabilité** des archives numériques. Il s'agit de la **confidentialité**, de l'**intégrité**, de la **disponibilité**, de la **traçabilité** et de l'**authentification**. Chacun de ces piliers constitue un axe structurant de toute politique de cybersécurité appliquée à l'archivage électronique [13], [14].

Confidentialité

La confidentialité vise à restreindre l'accès aux documents uniquement aux personnes autorisées. Dans un SAE, cette exigence est essentielle, dans la mesure où les documents archivés peuvent contenir des informations sensibles sur les plans juridique, administratif, financier ou personnel. Pour assurer cette confidentialité, plusieurs mesures techniques sont mises en œuvre : **contrôle d'accès** par profil utilisateur, **cloisonnement des rôles**, **chiffrement des données** sensibles à l'aide d'algorithmes cryptographiques robustes, ou encore l'**anonymisation** partielle dans les cas spécifiques de données à caractère personnel. Le Règlement général sur la protection des données (RGPD) impose par ailleurs un haut niveau de protection pour toute information nominative, ce qui fait de la confidentialité un impératif légal [15]. L'ANSSI recommande à ce titre l'usage de méthodes d'authentification renforcée et de séparation des environnements à droits limités pour prévenir les fuites ou les accès illicites [16].

Intégrité

L'intégrité garantit qu'un document archivé n'a subi aucune altération, volontaire ou accidentelle, depuis son dépôt dans le SAE. Elle est le fondement même de la valeur probatoire des documents numériques. Pour y répondre, les SAE intègrent des dispositifs comme le calcul **d'empreintes numériques** (fonction de hachage de type SHA-256), l**'horodatage** certifié, ou la **signature électronique**. Ces mécanismes permettent, en cas de vérification, de démontrer que le fichier conservé est identique à sa version d'origine. La norme NF Z42-013, de même que le règlement (UE) 2024/1183, exigent la mise en place de tels dispositifs, y compris la vérification automatisée de la conformité des documents lors de leur restitution, afin d'assurer une continuité de preuve dans le temps [10], [17].

Disponibilité

La disponibilité suppose que les documents archivés soient accessibles en permanence aux ayants droits autorisés, pendant toute leur durée de conservation. Cette exigence prend une

importance particulière dans les contextes où la durée légale de conservation peut atteindre plusieurs décennies, voire être illimitée pour les archives patrimoniales. Pour garantir cette disponibilité, les SAE doivent intégrer des stratégies de **redondance** (duplication sur plusieurs serveurs ou sites), des **plans de reprise d'activité** en cas de sinistre (PRA), et des procédures de **sauvegarde** régulières. L'usage de **formats pérennes** (PDF/A, XML, TIFF…) et interopérables est également requis pour prévenir l'inaccessibilité liée à l'obsolescence technologique. Ainsi, la disponibilité n'est pas simplement une question d'accès immédiat, mais de résilience structurelle dans le temps long [13].

Traçabilité

La traçabilité permet de reconstituer l'historique complet des opérations effectuées sur les documents archivés. Elle concerne aussi bien les actions techniques (versements, consultations, modifications, suppressions) que les évolutions du système ou les interventions des administrateurs. Pour garantir cette traçabilité, les SAE s'appuient sur un système de **journalisation sécurisé** (logs), qui consigne chaque événement dans des **journaux scellés**, parfois même chaînés (comme la blockchain). Ces journaux doivent eux-mêmes être conservés à long terme, dans des conditions qui empêchent toute altération ou suppression. La norme **ISO 14721 (OAIS)** identifie la gestion de ces journaux comme une composante fonctionnelle essentielle, tandis que les recommandations de l'**ANSSI** insistent sur leur intégrité, leur accessibilité et leur exploitabilité en cas d'audit [16].

Authentification

L'authentification vise à garantir que toute opération réalisée dans le SAE est effectuée par une **personne autorisée**, clairement identifiée. Cette exigence implique le recours à des mécanismes d'identification adaptés au niveau de sensibilité des documents : **identifiants/mots de passe robustes**, **authentification multifacteur (MFA)**, **certificats numériques**, voire **identification biométrique** dans certains contextes. Dans le cadre d'un SAE qualifié, ces dispositifs doivent répondre aux standards du règlement eIDAS, qui encadre l'identification électronique et les services de confiance à l'échelle européenne. Le but est de pouvoir soumettre tout utilisateur au principe de non-répudiation. A travers le principe de répudiation ou d'imputation, les textes exigent une identification claire de l'utilisateur afin que « chacun demeure responsable des actes qu'il a réalisés » [14]. Par ailleurs, l'authentification peut aussi être appliquée au document lui-même : une **signature électronique qualifiée**, fondée sur un

certificat délivré par une autorité de confiance, permet d'attester formellement l'identité de son auteur, tout en renforçant la valeur juridique du document archivé [13].

Ainsi, ces cinq principes de **confidentialité, d'intégrité, de disponibilité, de traçabilité et d'authentification** ne sont pas de simples bonnes pratiques. Ils constituent les pré-requis techniques et normatifs d'un SAE conforme et sécurisé. Leur mise en œuvre, rigoureuse et systématique, conditionne non seulement la conformité réglementaire du système, mais aussi la confiance organisationnelle et juridique dans la pérennité des archives électroniques conservées.

2.2 Architecture sécurisée d'un SAE

La protection des archives numériques ne peut être assurée sans une architecture technique rigoureusement pensée, conçue pour anticiper les risques et garantir la robustesse du système sur le long terme. Dans un système d'archivage électronique (SAE), la sécurité n'est pas l'apanage d'un seul composant ; elle repose au contraire sur un agencement cohérent de ressources matérielles, logicielles et organisationnelles, visant à prévenir toute altération, perte ou divulgation non autorisée des documents conservés. L'objectif fondamental de cette architecture est double : garantir la continuité de l'accès aux archives dans le temps, et préserver leur intégrité et leur valeur probante malgré l'évolution des menaces ou des technologies.

« Les archives électroniques font partie du SI de la collectivité, il s'agit de données comme les autres qui bénéficient donc du même socle commun de sécurisation. À ce socle commun se greffe un niveau d'exigence supérieur, adapté à la conservation des archives. Les volumes dédiés aux archives électroniques contiennent également les fonds d'archives numérisés. »[18]

La première exigence structurante d'un SAE sécurisé réside dans l'**isolement de ses ressources critiques**, à travers une segmentation rigoureuse des réseaux et des environnements. Des mesures de défense en profondeur sont déployées, combinant pare-feux (firewalls), antivirus, systèmes de détection et de prévention d'intrusion (IDS/IPS), ainsi que des politiques de durcissement des postes et de gestion centralisée des correctifs. Ces dispositifs réduisent la surface d'exposition du système aux attaques et assurent une protection contre les programmes malveillants et les accès non autorisés [13].

La **sécurisation du stockage** constitue un second pilier fondamental. Elle implique l'utilisation de serveurs dédiés, d'environnements virtualisés cloisonnés ou de solutions hybrides, accompagnés de mécanismes de réplication inter-sites, de sauvegardes régulières et de redondance physique. Ce modèle, conforme à l'architecture fonctionnelle du standard OAIS (ISO 14721), permet de maintenir l'accessibilité des archives en cas de sinistre, de panne ou d'incident majeur.

L'**encadrement des accès** repose quant à lui sur une gestion fine des identités et des habilitations, définies en fonction des rôles (producteur, lecteur, administrateur) et des niveaux de sensibilité des documents. Ce dispositif est complété par une authentification forte avec des mots de passe complexes, une authentification à deux facteurs (2FA) ou un certificat électronique notamment pour les opérations critiques. Ces pratiques sont essentielles pour prévenir toute compromission liée à l'usurpation d'identité ou aux accès non tracés [19].

En parallèle, la **traçabilité des opérations** constitue un élément central de l'architecture sécurisée. Elle repose sur un système de journalisation détaillé, horodaté, et protégé contre toute modification. Ces journaux d'audit conservent la mémoire des versements, consultations, modifications ou suppressions, et sont indispensables pour répondre aux exigences probatoires des normes telles que NF Z42-013 et ISO 27001 [20].

Les documents eux-mêmes sont encapsulés dans des **paquets d'archives structurés selon le standard SEDA**, intégrant contenus, métadonnées, empreintes et règles de gestion. Le SEDA (Standard d'Échange de Données pour l'Archivage) est un référentiel normatif conçu pour garantir l'interopérabilité entre le système d'information d'un service d'archives et ceux de ses partenaires. Il permet de formaliser l'ensemble des transactions liées à l'archivage numérique qu'il s'agisse de transfert, de modification, d'élimination ou de restitution de données en définissant clairement les formats, l'ordre et la nature des messages échangés [21]. Cette structuration facilite les contrôles d'intégrité automatisés, la migration des données et l'interopérabilité avec d'autres systèmes archivistiques ou de gestion documentaire.

Enfin, les SAE les plus avancés recourent à des **technologies de sécurité renforcée**, telles que les modules cryptographiques matériels (HSM), les horodateurs qualifiés ou, plus récemment, les mécanismes de preuve fondés sur la blockchain. Ces outils permettent d'ajouter une couche de vérifiabilité et d'inviolabilité aux documents à forte valeur juridique ou sensible.

Ces dispositifs forment un socle de protection robuste, complété par des mécanismes de preuve numérique que nous présentons à présent. La mise en place de **mesures de défense en profondeur**, combinée à une **sécurisation du stockage** et une **gestion stricte des accès**, permet de prévenir les risques de compromission ou de perte. Le recours à des standards tels que **SEDA** et **OAIS** assure l'interopérabilité des systèmes archivistiques, tandis que les technologies avancées comme la **blockchain** et les **HSM** renforcent la fiabilité et la pérennité des archives électroniques. En intégrant ces principes, les organismes peuvent garantir une conservation sécurisée des documents tout en répondant aux exigences normatives et aux défis futurs du numérique

2.3 Cas particuliers : signature électronique, horodatage, empreinte numérique

La mise en œuvre d'un système d'archivage électronique (SAE) conforme aux exigences de fiabilité et de légalité suppose l'intégration de mécanismes techniques spécifiques destinés à renforcer la **valeur juridique, la traçabilité et l'intégrité** des documents numériques. Parmi ces dispositifs, trois outils occupent une place centrale : la **signature électronique**, l'**horodatage** et l'**empreinte numérique**. Loin d'être des fonctionnalités accessoires, ils constituent le socle technologique d'une politique d'archivage à valeur probatoire.

La **signature électronique** est un mécanisme de sécurité qui permet de garantir l'authenticité d'un document ainsi que l'identité de la personne qui l'a signé. Pour ce faire, elle ne se contente pas d'apposer une image ou une représentation d'une signature manuscrite ; elle crée plutôt un lien cryptographique avec le contenu du document. Concrètement, elle repose sur des mécanismes de chiffrement asymétrique fondés sur des clés et un certificat numérique, garantissant l'identité du signataire et l'intégrité du document.

L**e** règlement eIDAS (UE n° 910/2014)**,** renforcé par le règlement (UE) 2024/1183, distingue trois niveaux de signature : **simple**, **avancée**, et **qualifiée**. Cette dernière, seule à bénéficier d'une présomption de fiabilité juridique équivalente à celle d'une signature manuscrite, doit être produite à l'aide d'un dispositif sécurisé certifié et délivrée par un **prestataire de services de confiance qualifié** [10].

Dans un contexte archivistique, la signature électronique permet de **figer un contenu** à un moment précis, en empêchant toute modification ultérieure sans détection. Elle est un instrument essentiel de **non-répudiation**, car une tentative d'altération rend la signature

invalide. Elle peut également servir à **signer un lot d'archives**, un **journal d'événements**, ou encore une **preuve de versement**, augmentant ainsi le niveau de traçabilité du SAE [27].

L'**horodatage électronique** quant à lui, est un mécanisme permettant d'associer à un document une **date et une heure**. On peut également parler d'horodatage qualifiée lorsqu'il est fourni par un **tiers de confiance indépendant**. Il garantit que le document existait bien dans un état donné à une date précise, indépendamment du système d'origine ou de l'utilisateur. L'horodatage repose généralement sur un **jeton temporel (**une donnée sécurisée qui certifie qu'un document ou une transaction existait à un moment précis) apposé au document, scellé par un service d'horodatage habilité.

Ce mécanisme joue un rôle déterminant dans les contextes où la **preuve de l'antériorité** est requise : respect de délais réglementaires, validation de contrats, opposition à des litiges. Dans un SAE, l'horodatage est souvent associé à la signature électronique pour renforcer la chaîne de confiance : il permet de **certifier le moment de signature** et d'en garantir la **pérennité juridique**.

Le concept d'**empreinte numérique** (ou *hash*) renvoie à une valeur unique générée à partir du contenu d'un fichier, grâce à une **fonction de hachage cryptographique** (telle que SHA-256 ou SHA-3). Elle agit comme une **empreinte digitale du document** : toute modification, même minime, entraîne une empreinte radicalement différente, ce qui permet de détecter immédiatement toute altération.

Dans les SAE, l'empreinte est généralement calculée lors du dépôt**,** puis archivée dans les métadonnées ou les journaux de traçabilité. Elle peut être vérifiée à intervalles réguliers ou lors de la restitution du document afin d'attester de son intégrité. Cette exigence est au cœur de la norme NF Z42-013, qui impose que l'intégrité des documents soit vérifiable tout au long de leur cycle de conservation [27].

Ces trois mécanismes sont souvent intégrés dans des solutions combinées au sein des SAE qualifiés. Certains prestataires proposent des jetons de preuve cryptographique**,** qui regroupent signature, empreinte et horodatage dans un format unique, scellé et horodaté. Ce type de solution permet d'automatiser le processus de contrôle de conformité, de faciliter les audits et de garantir une traçabilité infalsifiable du cycle de vie des documents.

Le **règlement (UE) 2024/1183** exige d'ailleurs que les systèmes qualifiés soient en mesure de générer et vérifier automatiquement ces preuves techniques, notamment lors de l'extraction ou de la restitution des documents. La chaîne de confiance doit ainsi être continue, documentée et sécurisée, sans rupture entre la création du document, sa conservation, et son éventuelle utilisation à des fins probatoires.

En conclusion, la signature électronique**,** l'horodatage et l'empreinte numérique représentent les piliers techniques de la preuve numérique dans un SAE. Leur intégration cohérente et leur exploitation rigoureuse permettent de garantir la valeur juridique, la transparence et la pérennité des documents archivés. À l'heure des cybermenaces croissantes et des exigences réglementaires renforcées, ces mécanismes s'imposent comme des composantes incontournables d'une stratégie d'archivage électronique robuste et conforme.

2.4 Réglementation et gouvernance de la sécurité

La sécurisation des SAE ne peut être abordée uniquement sous un prisme technique. Elle s'inscrit dans un cadre réglementaire, normatif et organisationnel multiscalaire, qui vise à garantir la conformité des dispositifs aux exigences légales, tout en instaurant une gouvernance de la sécurité structurée et dynamique.

Le **règlement (UE) 2024/1183** constitue une avancée majeure dans la régulation des services de confiance pour les transactions électroniques, en particulier l'archivage électronique qualifié. Les prestataires certifiés doivent démontrer leur capacité à assurer une **restauration fidèle** des documents et à maintenir un historique complet des traitements effectués. La **certification obligatoire** par une autorité de contrôle confère une présomption de validité juridique aux archives numériques, facilitant leur reconnaissance dans le cadre juridique européen. Ce règlement souligne l'importance d'une infrastructure robuste et sécurisée pour préserver la fiabilité des archives à long terme

Le **RGPD (Règlement Général sur la Protection des Données**) impose des obligations strictes aux systèmes d'archivage électronique (SAE) dès lors qu'ils contiennent des données personnelles. Voici quelques éléments clés à comprendre :

- **Principe de licéité et limitation des finalités** : Les données doivent être collectées et traitées dans un cadre légal précis, et uniquement pour des objectifs clairement définis.

Cela signifie qu'un SAE doit s'assurer que toutes les informations qu'il héberge ont été recueillies pour des finalités légitimes et ne seront utilisées que dans ce cadre.

- **Minimisation des données** : Il est nécessaire de ne conserver que les informations strictement indispensables aux finalités fixées. Pour un SAE, cela implique une gestion fine des données stockées, en éliminant tout élément superflu ou non pertinent.
- **Mesures de sécurité dès la conception (Privacy by Design)** : Dès la phase de conception du système, des dispositifs techniques et organisationnels doivent être intégrés pour protéger les données contre tout accès non autorisé, altération ou perte. Cette intégration préventive est cruciale pour assurer la pérennité et la fiabilité des archives.

- **Analyse d'impact sur la protection des données** : Avant la mise en place ou lors de modifications majeures d'un SAE, une analyse d'impact doit être réalisée pour évaluer les risques pesant sur les droits et libertés des personnes concernées. Cela permet d'identifier les vulnérabilités potentielles et de mettre en œuvre des mesures correctives adaptées.
- **Registre des traitements** : Les gestionnaires de SAE doivent tenir à jour un registre qui documente l'ensemble des traitements réalisés sur les données personnelles. Ce registre est indispensable pour démontrer la conformité du système et pour faciliter la traçabilité des opérations.
- **Notification des violations de données** : En cas de faille ou d'incident entraînant la compromission des données, le RGPD impose une obligation de notifier l'incident aux autorités compétentes (et aux personnes concernées, si nécessaire) dans un délai très court (souvent 72 heures). Cela oblige les responsables des SAE à mettre en place des procédures réactives et transparentes pour gérer et remédier aux incidents [22], [23].

En réunissant ces mesures, le système d'archivage électronique ne se contente pas seulement de stocker des données, il garantit également que celles-ci restent protégées, conformes aux exigences légales et respectueuses des droits individuels tout au long de leur cycle de conservation. Cela conforte la confiance des usagers et assure que le traitement des informations est sûr et traçable.

Le **Code du patrimoine et la loi du 15 juillet 2008** sur les archives fixent un cadre juridique strict pour la conservation des documents, qu'ils soient physiques ou numériques, présentant

une valeur patrimoniale ou administrative [2],[24]. Ces textes imposent que la conservation assure l'intégrité (les documents doivent rester intacts et non modifiés), la pérennité (leur accessibilité doit être garantie sur le long terme) et la communicabilité (la diffusion et le partage des informations doivent rester possibles) des archives. Ainsi, pour répondre à ces exigences élevées, notamment dans le contexte de la digitalisation, les administrations publiques et les organismes délégués de service public doivent se doter d'un Système d'Archivage Électronique (SAE) homologué. Ce type de système certifié garantit qu'un ensemble de critères techniques et organisationnels rigoureux est respecté, assurant une gestion fiable et pérenne des archives numériques, conforme aux prescriptions légales et aux besoins de vérification et de validité juridique des documents.

Quant à la norme **ISO/CEI 27001** un cadre international, elle est destinée à instaurer un Système de Management de la Sécurité de l'Information (SMSI) basé sur l'évaluation des risques. Elle impose aux organisations d'identifier, d'analyser et de traiter les menaces pesant sur leurs actifs informationnels (Humains, matériels et infrastructures). Cela passe par l'élaboration d'une politique de sécurité documentée, définissant des objectifs clairs et répartissant les responsabilités en matière de sécurité afin de garantir la confidentialité, l'intégrité et la disponibilité des informations. En application, la norme requiert la mise en œuvre de mesures de contrôle couvrant plusieurs domaines : des dispositifs organisationnels (sensibilisation, formation, gestion des accès), techniques (chiffrement, contrôle d'accès, sauvegardes) et physiques (sécurisation des locaux, contrôle des accès physiques). Elle s'appuie également sur un cycle d'amélioration continue (Planifier, Réaliser, Vérifier, Agir) permettant d'adapter en permanence les mesures de sécurité aux évolutions des menaces et des technologies, assurant ainsi une traçabilité complète des décisions et une robustesse pérenne des dispositifs de protection.

Dans le contexte d'un Système d'Archivage Électronique (SAE), l'application de cette norme permet de formaliser l'ensemble des processus de sécurisation, d'assurer la traçabilité des décisions prises et de démontrer la conformité du système face aux exigences normatives et réglementaires. La mise en œuvre d'ISO/CEI 27001 dans un SAE contribue ainsi à la robustesse et à la fiabilité du système, tout en garantissant la protection des données archivées sur le long terme à travers le triade CID (confidentialité, Intégrité, Disponibilité) [25],[26]. En France, l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information**)** joue un rôle normatif essentiel. Ses guides fournissent des recommandations concrètes sur la **protection des**

journaux, la **séparation des environnements sensibles**, la **gestion des vulnérabilités**, l'**authentification forte** ou la **supervision continue**. Ces orientations sont d'ailleurs de plus en plus intégrées aux appels d'offres et aux processus de certification.

En interne, la gouvernance de la sécurité repose sur des dispositifs opérationnels à savoirs : une politique de sécurité du système d'information (PSSI)**,** des chartes d'utilisation**,** des comités de sécurité**,** des audits périodiques**,** et la désignation de référents tels que le Responsable de la sécurité des systèmes d'Information et /ou le Data Protection Officer. Ces fonctions assurent la cohérence des mesures de sécurité, leur déclinaison dans les processus métiers, et leur suivi dans le temps. Elles doivent impérativement collaborer avec les responsables des SAE pour assurer une vision transversale de la sécurité documentaire**.**

En définitive, la gouvernance de la sécurité dans les SAE repose sur l'interdépendance entre cadre réglementaire, stratégie organisationnelle et dispositifs opérationnels. Elle constitue un levier stratégique majeur, garantissant la confiance dans les systèmes, la conformité légale, et la résilience des institutions face aux risques numériques croissants.

Ce chapitre a mis en évidence les fondements de la sécurité appliquée aux systèmes d'information et, plus spécifiquement, aux systèmes d'archivage électronique (SAE). À travers l'analyse des cinq principes essentiels : confidentialité, intégrité, disponibilité, traçabilité et authentification, il apparaît que la sécurité des SAE repose sur une combinaison rigoureuse de dispositifs techniques, d'exigences réglementaires et de pratiques organisationnelles. L'architecture sécurisée du système, la conformité aux normes comme ISO 27001 ou NF Z42-013, ainsi que la mise en œuvre de mécanismes spécifiques tels que la signature électronique ou l'horodatage, constituent autant de garanties indispensables. Toutefois, malgré cette structuration, les SAE restent vulnérables à des menaces qui dépassent les seules logiques de conformité. Le chapitre suivant se penchera ainsi sur les risques émergents, afin de dresser une cartographie des cybermenaces susceptibles d'affecter la fiabilité de ces dispositifs.

Chapitre 3 - Menaces émergentes et vulnérabilités des SAE

Les systèmes d'archivage électronique (SAE), pourtant conçus pour assurer la pérennité et l'intégrité des documents numériques, se trouvent exposés à des menaces de plus en plus sophistiquées. La montée en puissance des cyberattaques ciblées, l'exploitation de vulnérabilités logicielles, l'usage détourné de l'intelligence artificielle ou encore les risques

d'obsolescence technique fragilisent la sécurité des archives conservées. Ce contexte soulève une problématique centrale : quelles sont les menaces spécifiques pesant aujourd'hui sur les SAE, et quelles en sont les implications en termes de vulnérabilités systémiques et documentaires ? Ce chapitre dresse une cartographie des cybermenaces actuelles, s'appuie sur des situations récentes pour illustrer les failles concrètes observées, et analyse les risques liés à la pérennité technologique ainsi que les usages ambivalents de l'IA.

3.1 Cartographie des cybermenaces

Malgré leur vocation première de conservation pérenne, intègre et sécurisée des documents numériques, les systèmes d'archivage électronique (SAE) ne sont plus à l'abri des dynamiques hostiles qui caractérisent le cyberespace. Le renforcement des exigences en matière de cybersécurité s'explique par l'évolution rapide, polymorphe et souvent imprévisible des cybermenaces. Ces attaques ne sont plus de simples hypothèses théoriques : elles affectent désormais concrètement les institutions publiques, les entreprises privées et les prestataires d'archivage. La cartographie des cybermenaces applicables aux SAE que nous exposerons ainsi a pour but d'identifier les vecteurs de risque dominants et de guider la conception de défenses adaptées.

Tous les environnements numériques, y compris les bases de données hébergées en cloud ou sur site, même lorsqu'ils intègrent des dispositifs de sécurité comme un coffre-fort numérique, ne répondent pas nécessairement aux exigences normatives, fonctionnelles et archivistiques qui définissent un SAE au sens strict. En revanche, en raison de leur rôle central dans le traitement et la conservation de l'information, ces infrastructures sont bel et bien exposées aux risques de cyberattaques que nous allons présenter ci-après.

Le rançongiciel (ransomware) : une menace prédatrice et persistante

Le **rançongiciel** demeure aujourd'hui l'une des menaces les plus agressives et fréquentes. Cette attaque consiste à chiffrer les données du système visé pour ensuite réclamer une rançon en échange de la clé de déchiffrement. Les années 2023 et 2024 ont enregistré les taux les plus élevés (66% et 59%) de ransomwares, introduits via des vulnérabilités non corrigées dans des composants tiers ou des configurations défaillantes [28]. Les SAE, de par leur rôle de gardiens d'informations critiques (dossiers juridiques, pièces financières, archives stratégiques) représentent donc de belles cibles en entreprises. Il a été plusieurs fois noté par exemple que le

ransomware «Ryuk […] a été utilisé que pour cibler les environnements d'entreprise »[29].Bien que les attaques spécifiques contre des SAE ne soient pas toujours largement documentées, les ransomwares touchent souvent des institutions qui gèrent des données critiques. Détecté en février 2024 par exemple, « RansomHub exploite les vulnérabilités dans les sauvegardes de stockage cloud et les instances Amazon S3 mal configurées, tirant parti de la confiance entre les fournisseurs et les clients pour améliorer leurs tactiques d'extorsion » [30].

L'hameçonnage (phishing) : vecteur d'usurpation et d'infiltration

Les attaques par **hameçonnage**, bien qu'issues d'une stratégie sociale plutôt que technique, restent redoutablement efficaces. Elles consistent à inciter un utilisateur à révéler ses identifiants via un faux message ou une interface usurpée [31]. Dans un contexte d'archivage, la compromission d'un **compte disposant de privilèges d'accès** peut permettre à un attaquant de consulter, modifier ou supprimer des documents sensibles. Cette intrusion compromet directement la **traçabilité**, l'**authenticité** et la **valeur probatoire** des documents archivés.

Les APT (Advanced Persistent Threats) : attaques furtives et prolongées

Les menaces qualifiées d'**APT (Advanced Persistent Threats)** se caractérisent par une stratégie d'infiltration discrète, progressive et ciblée. Leur objectif n'est pas la destruction immédiate de données, mais l'**extraction continue et indétectée d'informations**. Les SAE, qui hébergent des documents à valeur sensible ou stratégique, peuvent constituer une cible d'intérêt pour ces attaques, notamment lorsqu'ils concernent des données sensibles d'États**,** de chercheurs, ou de structures culturelles. Une compromission silencieuse pourrait impacter non seulement les contenus, mais aussi les journaux d'audit, les métadonnées, voire les clés de signature. **APT28**, aussi connu sous les noms **Fancy Bear**, **Sofacy** ou **STRONTIUM**, est un groupe de cyberespionnage qui correspond bien à la définition d'une **Advanced Persistent Threat (APT)**. Ce groupe est attribué à l'agence de renseignement militaire russe **GRU** et est actif depuis au moins **2004 [31].**

Les failles logicielles : vulnérabilités systémiques

Les vulnérabilités exploitées par les cybercriminels proviennent souvent de **failles non corrigées dans les logiciels** ou dans les composants intégrés aux SAE. Ces failles peuvent

résider dans les bibliothèques logicielles, les serveurs d'application, les interfaces d'administration, ou encore dans les protocoles de communication. L'affaire **MOVEit**, largement médiatisée en 2023, a démontré qu'un simple **outil de transfert de fichiers** pouvait servir de porte d'entrée à des exfiltrations massives de données, même dans des environnements censés être étanches [32].

L'IA : à la fois menace et opportunité

L'**intelligence artificielle (IA)** joue un rôle ambivalent dans la cybersécurité des SAE. Elle peut être mobilisée par des attaquants pour générer des **faux documents crédibles** (deepfakes documentaires), automatiser des campagnes d'hameçonnage contextuel, ou contourner des mécanismes de détection classiques. Parallèlement, l'IA offre aussi des opportunités défensives : analyse comportementale des accès, détection de variations anormales, réaction automatisée en cas de tentative d'intrusion. L'intégration de ces technologies dans les SAE reste néanmoins limitée et nécessite une gouvernance éthique et transparente.

Mauvaises configurations : la menace silencieuse des erreurs humaines

Au-delà des failles techniques, certains incidents trouvent leur origine dans des **configurations** inappropriées, souvent dues à une méconnaissance des mécanismes de sécurité. Ces erreurs exposent des documents confidentiels à des consultations non autorisées, compromettant leur valeur juridique et leur **c**onfidentialité ; ce qui rappellent l'importance d'une vigilance organisationnelle continue et d'une gouvernance partagée entre responsables IT, archivistes et gestionnaires de risques.

Ces différents incidents démontrent que les SAE, même adossés à des normes strictes et à des prestataires certifiés, ne sont pas hermétiques aux cybermenaces. Leur interconnexion croissante**,** leur dépendance à des solutions tierces, et leur complexité organisationnelle en font des cibles potentielles pour des attaques variées ciblées, opportunistes ou accidentelles. Dès lors, il est impératif de renforcer à la fois les dispositifs techniques de protection, mais aussi la gouvernance, la supervision et la formation des utilisateurs.

Ces retours d'expérience plaident en faveur d'une stratégie de cybersécurité intégrée aux SAE, articulant anticipation, détection**,** résilience**,** et réversibilité, afin d'assurer la continuité des services d'archivage**,** et la confiance durable dans la préservation numérique.

Les menaces internes qu'elles relèvent de la **malveillance**, de la **négligence** ou d'un **manque de formation** constituent une source fréquente d'incidents de sécurité. Une suppression accidentelle, une mauvaise gestion des habilitations ou le partage involontaire d'un identifiant peuvent suffire à compromettre un fonds documentaire entier. La voix des acteurs de la cybersécurité est unanime : L'humain reste la première faille de nos systèmes de sécurité. Dans un SAE, la gestion du cycle de vie des utilisateurs, la limitation des privilèges, ainsi que la sensibilisation continue du personnel sont donc autant de leviers de prévention indispensables.

La cartographie des menaces applicables aux SAE met en lumière une **multiplicité de vecteurs d'attaque**, allant des plus directs (ransomwares, exploitation de failles) aux plus insidieux (APT, erreurs humaines). Cette diversité impose une approche de sécurité intégrée et évolutive, ancrée dans la vigilance permanente**,** la mise à jour continue des systèmes, et une politique de gouvernance proactive.

3.2 Études de cas de cyberattaques récentes touchant des administrations

L'évolution des menaces informatiques a contribué à faire des systèmes d'archivage électronique (SAE) des cibles non plus hypothétiques, mais bien opérationnelles et prioritaires pour les cyberattaquants. De récents incidents, touchant aussi bien les infrastructures publiques que les systèmes documentaires privés, illustrent la vulnérabilité croissante des environnements d'archivage interconnectés. Ces exemples concrets permettent de mieux cerner les **vecteurs d'intrusion**, les **failles exploitées**, et les **conséquences directes** sur la sécurité des documents numériques.

Faille critique dans Fortinet : compromission des protections périmétriques

En février 2024, une **vulnérabilité critique** (CVE-2023-27997) fut identifiée dans les pare-feux FortiGate de l'entreprise **Fortinet**, largement utilisés par les administrations françaises pour assurer une gestion unifiée des menaces de leur cyberespaces. Cette faille permettait l'exécution de **code malveillant à distance**, ouvrant ainsi la voie à des **prises de contrôle complètes** de dispositifs de sécurité pourtant certifiés. Ce qui a affecté près de 0,3% de leurs clients. Les données volées ont été rendues publiques par les pirates après le refus de l'entreprise de payer une rançon. Cependant, Fortinet a assuré que les opérations et les services n'ont pas été compromis, et des mesures ont été prises pour renforcer la sécurité et éviter que cela ne se

reproduise. Ce cas souligne les risques associés à la dépendance vis-à-vis de composants périmétriques extérieurs aux SAE eux-mêmes, mais essentiels à leur protection [33].

MOVEit : une vulnérabilité indirecte aux effets massifs

Le cas **MOVEit**, survenu en 2023, illustre la portée systémique que peut prendre une vulnérabilité isolée. MOVEit est un logiciel de transfert de fichiers sécurisé développé par Progress Software. Il permet aux entreprises de gérer et sécuriser leurs échanges de données, notamment via le cloud et des flux automatisés. Cependant, MOVEit a été victime d'une faille de sécurité en mai 2023, exploitée par des hackers du groupe Clop, entraînant la compromission de milliers d'entreprises. La faille (ingestion SQL) exploitée par le groupe **Cl0p** a conduit à une fuite massive d'informations confidentielles**,** incluant données RH**,** relevés bancaires **ou** archives fiscales. Ce cas démontre que les SAE peuvent être compromis sans attaque directe, mais via les flux de données alimentant leur contenu. Plusieurs institutions publiques françaises ont ainsi vu leurs archives exposées du fait d'une dépendance logicielle mal maîtrisée [32]. Le groupe Cl0p a mené une campagne très structurée, visant des milliers d'organisations dans le monde, dont certaines en **France**, comme **Synlab** et **Cegedim**, deux acteurs du secteur de la santé et des services numériques[34].Ce cas illustre parfaitement le risque de **compromission indirecte** des SAE : même si le système d'archivage n'est pas attaqué directement, les **flux de données entrants** (comme ceux gérés par MOVEit) peuvent devenir des vecteurs d'intrusion si les outils intermédiaires sont vulnérables.

Cyberattaque sur les collectivités territoriales : La région Grand Est et l'agglomération Grand Cognac

L'**agglomération Grand Cognac a** été victime d'une cyberattaque par rançongiciel, rendant toutes ses données informatiques inaccessibles (illisibles). Survenue la nuit du 11 au 12 octobre 2019, « Cette cyberattaque a atteint son serveur principal, celui de secours et de sauvegardes. Résultat : des milliers de fichiers contaminés, illisibles, et notamment tout ce qui touche à l'urbanisme, aux particuliers et aux entreprises comme les permis de construire, les enquêtes et marchés publics » [35]. Grâce à un virus les pirates ont profité d'une faille dans le système de messagerie avant de s'attaquer aux ordinateurs de la collectivité. Ces derniers ont ensuite exigé une rançon de 180 000 euros en échange des clés de décryptage, mais les autorités locales ont rejeté cette proposition.

Quant à la **région Grand Est**, elle a été confrontée à une cyberattaque qui a paralysé **80 serveurs en 2021**. Cette attaque, sous forme de **rançongiciel**, a chiffré les données du réseau, les rendant inaccessibles. Les postes de travail étaient toujours accessibles. Les hackers ont surtout principalement visé les serveurs. Concernant les données perdues ou compromises, il est difficile de déterminer précisément l'ampleur des fuites. Les autorités ont refusé de payer la rançon et ont travaillé à la restauration des systèmes à partir de sauvegardes. Toutefois, les systèmes affectés incluaient des **applications métiers et des outils de bureautique** utilisés par les employés [36]. Au regard de tout ce que nous avons étudié autour de ce sujet, nous pouvons déduire que le SAE du Grand Est a dû être également impacté par cette attaque.

L'analyse des cyberattaques récentes démontre que les Systèmes d'Archivage Électronique, bien qu'ils ne soient pas toujours la cible première des cybercriminels, subissent néanmoins des impacts directs ou indirects en raison des vulnérabilités des infrastructures numériques qui les hébergent. Que ce soit par des **failles périmétriques** (cas Fortinet), des **vulnérabilités sur des flux de transfert de données** (MOVEit) ou des **attaques par rançongiciel** ciblant des administrations publiques (Grand Est), ces incidents montrent que les SAE ne sont pas à l'abri des risques informatiques. L'absence de documentation spécifique sur les cyberattaques visant directement les SAE ne signifie pas qu'ils sont protégés, mais plutôt qu'ils sont souvent victimes d'attaques indirectes via les systèmes interconnectés qui leur permettent de fonctionner.

3.3 Vulnérabilités liées à l'obsolescence technologique et à la pérennité des formats

Parmi les risques les plus insidieux affectant les systèmes d'archivage électronique (SAE), les vulnérabilités liées à l'obsolescence technologique et à la non-pérennité des formats occupent une place centrale. À la différence des attaques directes, ces menaces s'inscrivent dans une logique temporelle silencieuse, mais potentiellement dévastatrice : elles compromettent la **l**isibilité, la compréhension et la réutilisabilité des documents archivés, parfois de manière irréversible. L'archivage à long terme est particulièrement exposé à cette obsolescence, quand les formats ou logiciels deviennent inexploitables.

L'**obsolescence technologique** se définit comme l'incapacité progressive d'un système matériel ou logiciel à prendre en charge, lire ou interpréter des contenus anciens, en raison de l'évolution des standards, des protocoles ou des environnements techniques. Dans un SAE, cette vulnérabilité peut concerner à la fois les **formats de fichiers**, les **systèmes d'exploitation**,

les **langages de programmation**, ou les **supports physiques** (tels que disques durs, bandes magnétiques ou serveurs virtualisés). Un document archivé peut ainsi devenir **illisible** faute d'un **logiciel compatible**, ou d'un **format abandonné** par son éditeur d'origine.

Cette fragilité est aggravée par le recours courant à des **formats propriétaires**, notamment ceux générés par des outils bureautiques ou applicatifs métiers. Bien que les SAE essaient d'éviter ce problème en soumettant la majorité des données à des formats standard pour la conservation, nous ne sommes jamais bien loin d'une obsolescence de format. Nous devons donc garder à l'esprit qu'un format de fichier devenu illisible empêche toute vérification de son authenticité et peut masquer des manipulations non détectées. De plus, l'utilisation de logiciels abandonnés pour lire ces formats pose un risque de sécurité : un programme obsolète peut contenir des failles exploitables par des attaquants. En cas de perte d'accès à un document, les institutions peuvent être contraintes de recourir à des outils tiers ou à des spécialistes, mettant en péril la confidentialité des données archivées. Enfin, l'incapacité à garantir l'accès à ces documents peut entraîner des **problèmes de conformité réglementaire**, compromettant des obligations légales de conservation.

Le **modèle OAIS (ISO 14721)** identifie explicitement la **planification de la préservation** comme une fonction essentielle du SAE. Il s'agit non seulement de stocker les documents, mais de **prévoir les évolutions futures de l'écosystème technique** afin de garantir leur accessibilité continue. Cela implique une **surveillance active des formats sensibles**, l'identification des **risques d'obsolescence**, et la capacité à engager des **actions de migration**, de **conversion** ou d'**émulation**, sans altérer les contenus ni les métadonnées. Ce pilotage stratégique doit être intégré aux politiques de gestion documentaire dès la conception du système [5].

Tout ceci nous fait prendre conscience de la fragilité des logiciels d'archivage eux-mêmes. L'obsolescence concerne également les **composants des SAE**. Un logiciel non maintenu, un module tiers abandonné, ou une dépendance technologique non compatible avec les futures versions de l'environnement peuvent affaiblir la chaîne de conservation.

3.4 L'intelligence artificielle : risque émergent ou levier défensif pour les SAE ?

L'irruption de l'**intelligence artificielle (IA)** dans le champ de la cybersécurité modifie en profondeur les paradigmes de protection des systèmes d'information, y compris ceux dédiés à l'archivage électronique. Initialement conçue comme un outil d'automatisation et

d'optimisation des processus, l'IA est aujourd'hui à la fois un vecteur d'innovation défensive et un facteur de risque émergent lorsqu'elle est utilisée de manière malveillante. Dans le contexte des **systèmes d'archivage électronique (SAE)**, cette dualité soulève des enjeux spécifiques, en raison de la valeur stratégique, juridique et patrimoniale des documents conservés.

L'un des apports majeurs de l'intelligence artificielle réside dans sa capacité à analyser de très grands volumes de données en temps réel, afin de détecter des anomalies comportementales et de prévenir des intrusions complexes**.** Dans un SAE, cela se traduit par la possibilité d'examiner automatiquement les journaux d'audit**,** d'identifier des comportements utilisateurs inhabituels (multiplication des accès, suppressions massives, requêtes anormales), ou encore de **détecter** des altérations documentaires difficilement repérables par les outils classiques [37].

Cependant, les capacités offertes par l'IA ne sont pas uniquement mobilisées à des fins de sécurité. Elles sont également exploitées dans le cadre **d'**attaques de nouvelle génération, caractérisées par leur vitesse d'exécution, leur précision contextuelle, et leur difficulté d'attribution. Des modèles génératifs sont désormais capables de créer des faux documents crédibles**,** de rédiger des courriels de phishing personnalisés, ou de simuler des voix et visages pour contourner les mécanismes d'authentification biométrique [38].

Dans un SAE, ces menaces peuvent prendre des formes multiples : injection de documents falsifiés dans un flux documentaire, usurpation de l'identité archivistique d'un agent**,** modification imperceptible des métadonnées associées à un fichier, ou encore altération de journaux de traçabilité. Ces scénarios, s'ils ne sont pas détectés à temps, peuvent remettre en cause la **valeur** probante**,** la traçabilité et la confiance institutionnelle associées aux documents numériques.

Des outils permettant **de** simuler des signatures électroniques**, de** générer des fichiers frauduleux ou de s'insérer discrètement dans une chaîne documentaire peuvent être manipulés sans expertise avancée. Si les SAE ne disposent pas de mécanismes de vérification automatisée robustes ou de **contre-mesures basées sur des IA défensives**, ils deviennent particulièrement vulnérables à ces menaces.

En conclusion, l'intelligence artificielle apparaît comme une **technologie ambivalente** pour les SAE : elle offre des **possibilités inédites d'anticipation, de détection et de rationalisation**

des processus d'archivage, mais ouvre également la voie à des **menaces d'un nouveau type**, polymorphes et difficiles à contenir. La **résilience des SAE face à l'IA** dépendra de leur capacité à en faire un levier maîtrisé de confiance numérique, intégré dans une architecture globale conjuguant normes archivistiques**,** exigences juridiques **et** principes de cybersécurité adaptative.

Cette première partie de notre étude nous présente une vue d'ensemble de la position des SAE dans le cyberespace. L'examen des menaces émergentes et des vulnérabilités propres aux systèmes d'archivage électronique (SAE) nous a permis de mettre en lumière l'ampleur et la diversité des risques auxquels ces dispositifs sont désormais exposés. Rançongiciels, attaques par hameçonnage, menaces persistantes avancées (APT), exploitation de failles logicielles ou encore usages malveillants de l'intelligence artificielle constituent autant de vecteurs susceptibles de compromettre l'intégrité, l'accessibilité ou la traçabilité des archives numériques. À ces menaces s'ajoutent des fragilités plus structurelles, telles que l'obsolescence technologique ou la dégradation des formats, qui menacent la lisibilité même des contenus conservés à long terme. Ce panorama, à la fois technique et organisationnel, souligne les limites actuelles des approches défensives traditionnelles. Le chapitre suivant s'attachera dès lors à évaluer de manière critique les capacités réelles de défense des SAE, afin d'identifier les forces et les lacunes des dispositifs actuellement en place.

PARTIE II

Analyse critique et perspectives : vers une cybersécurisation durable des SAE

Après avoir établi les fondements théoriques, normatifs et techniques encadrant les systèmes d'archivage électronique (SAE), il convient désormais d'interroger leur capacité réelle à faire face aux défis opérationnels de la cybersécurité contemporaine. En effet, les exigences en matière de protection ne peuvent se limiter à des prescriptions réglementaires : elles doivent être confrontées à la réalité des usages, aux vulnérabilités observées sur le terrain, et à l'évolution rapide des menaces.

Cette deuxième partie adopte donc une approche critique et prospective. Elle vise à analyser la robustesse effective des dispositifs de défense des SAE, à évaluer leur agilité face aux environnements numériques complexes et interconnectés, et à identifier les leviers technologiques et organisationnels susceptibles d'améliorer leur résilience.

Malgré un encadrement normatif relativement structuré, les retours d'expérience récents y compris au sein d'institutions publiques ou de prestataires certifiés révèlent encore des failles préoccupantes, tant techniques que organisationnelles. La montée en puissance des attaques ciblées, la dépendance à des composants tiers, ainsi que les contraintes de continuité de service appellent une réévaluation des capacités adaptatives des SAE.

Cette analyse est structurée en trois chapitres. Le chapitre 4 propose une évaluation critique des dispositifs actuels de sécurisation et de sauvegarde, ainsi que des obstacles à leur adaptation. Le chapitre 5 explore les technologies émergentes blockchain, intelligence artificielle, systèmes d'identité et leur potentiel de renforcement sécuritaire. Enfin, le chapitre 6 formule des recommandations stratégiques pour une gouvernance résiliente de l'archivage numérique à l'ère des cybermenaces.

Chapitre 4 - Évaluation des capacités actuelles de défense des SAE

Dans un contexte où les exigences de cybersécurité s'intensifient et où les menaces se diversifient, les systèmes d'archivage électronique (SAE) doivent démontrer leur capacité effective à assurer la protection, la disponibilité et la résilience des archives numériques. Bien que encadrés par un ensemble de normes et de dispositifs techniques, leur efficacité opérationnelle demeure sujette à caution face à l'élévation constante du niveau de sophistication des attaques. Dès lors, une question centrale émerge : les SAE aujourd'hui en place disposent-ils de mécanismes de défense suffisamment robustes, flexibles et interopérables pour faire face à des cybermenaces toujours plus complexes ? Pour y répondre, ce chapitre propose une analyse critique des dispositifs de sécurité, des politiques de sauvegarde et des stratégies de continuité d'activité, tout en identifiant les limites structurelles auxquelles ces systèmes se heurtent. Afin de situer cette évaluation dans un cadre concret, l'analyse débute par la présentation de l'environnement organisationnel retenu comme terrain d'étude : **la société Congo Digital Service, filiale congolaise de l'entreprise Alessya Consulting.**

4.1 Présentation de Congo Digital Service, filiale congolaise de l'entreprise Alessya Consulting

Créée en mai 2024, Congo Digital Services (CDS) est une entreprise spécialisée dans le conseil et les systèmes informatiques opérant dans les villes de Brazzaville et de Pointe Noire de la République du Congo. Elle constitue une filiale opérationnelle d'Alessya Consulting, une société française fondée en 2019 par Fred Arly Kaya, dont les activités ont récemment repris pour se concrétiser autour de la conception de solutions numériques d'archivage à destination d'un public africain.

CDS se positionne comme un acteur de l'accompagnement numérique des institutions congolaises, tant publiques que privées. Ses domaines d'intervention couvrent le développement web et mobile, la dématérialisation, l'archivage électronique, la mise en œuvre de systèmes d'information (SIRH), le développement de solutions GED/SAE sur mesure, ainsi que la formation de professionnels de l'information documentaire. Forte d'une équipe de plus d'une dizaine de collaborateurs, l'entreprise articule ses services autour d'un rôle d'intégrateur technique et de conseiller stratégique en transformation numérique, au service des administrations centrales, collectivités territoriales, établissements parapublics ou encore structures privées en mutation numérique.

Dans le cadre du projet de développement d'un système d'archivage électronique et d'un logiciel GED, Alessya Consulting a sollicité une intégration à l'équipe projet de CDS. La mission confiée s'inscrivait dans la création d'une offre de services d'archivage, à la croisée de compétences en archivistique et en ingénierie de l'information numérique. À ce titre, un rôle de gestionnaire de projet informatique documentaire a été occupé, en accompagnement des développeurs dans la conception d'un SAE conforme aux exigences métier et réglementaires.

Très rapidement, il est apparu que la question de la sécurité des documents numériques constituait une préoccupation majeure pour les clients et partenaires sollicités. En effet, dans le contexte congolais, un cadre législatif strict impose que les données produites sur le territoire soient hébergées localement, en lien avec la mise en place récente d'un serveur national de stockage. Ce changement, bien qu'encourageant, soulève des incertitudes techniques et juridiques : méfiance vis-à-vis de l'infrastructure nationale, besoin de garanties de confidentialité, et interrogation sur les dispositifs de protection offerts dans les solutions GED-SAE en générales.

Ces interpellations récurrentes ont contribué à orienter la réflexion vers la problématique de la cybersécurité dans les systèmes d'archivage électronique, devenue l'axe central de ce mémoire. Dans cette perspective, il devient essentiel d'examiner de manière critique les dispositifs de sécurité actuellement intégrés aux systèmes d'archivage électronique, afin d'évaluer dans quelle mesure ils répondent concrètement aux exigences croissantes de cybersécurité.

L'ambition portée par Alessya Consulting dépasse d'ailleurs le seul cadre du Congo, considéré comme premier terrain d'expérimentation. L'entreprise entend se déployer progressivement dans la sous-région, notamment en Afrique centrale et en Afrique de l'Ouest (Togo, Côte d'Ivoire, Cameroun…), avec l'objectif de fournir des solutions résilientes et robustes, véritablement adaptées aux réalités locales. Celles-ci incluent notamment l'instabilité de la connexion, les difficultés d'accès à l'électricité, la diversité des infrastructures, et les contraintes budgétaires. L'enjeu est de proposer des systèmes qui ne se contentent pas d'imiter des modèles occidentaux, mais qui s'inscrivent dans une logique de durabilité, de sobriété et d'adaptation contextuelle.

4.2 Analyse critique des dispositifs existants

Les dispositifs de sécurisation présents dans les systèmes d'archivage électronique (SAE) actuels révèlent une conception rigoureuse du point de vue normatif et technique, mais leur mise en œuvre montre des limites importantes face aux menaces modernes. Ce décalage est apparu clairement au fil des entretiens menés, où les informaticiens interrogés ont reconnu l'efficacité des dispositifs classiques (chiffrement, journaux d'audit, redondance), tout en pointant des faiblesses concrètes dans leur adaptation aux cyberattaques contemporaines.

Par exemple, les SAE évalués reposent sur des mécanismes bien établis de journalisation des actions liées aux documents (modification, suppression, restitution). Ces logs sont horodatés, scellés et, dans certains cas, chaînés pour garantir leur intégrité. Cependant, il a été constaté que cette journalisation s'arrête à la couche documentaire : **les tentatives d'accès au système lui-même ne sont pas tracées**, et aucune alerte n'est déclenchée en cas d'échec répété de connexion. Cette lacune, confirmée dans au moins deux logiciels évalués, pose un problème majeur en matière de détection d'intrusion, car elle empêche toute supervision des comportements suspects sur l'interface d'accès.

Ce constat s'éloigne des recommandations de base de la cybersécurité, qui préconisent une journalisation étendue à toute activité système sensible, y compris les tentatives de connexion, même infructueuses [39]. L'absence de ces mesures empêche une détection précoce des attaques par force brute ou des compromissions de compte. Or, la compromission silencieuse d'un compte à privilège est aujourd'hui l'un des vecteurs d'attaque les plus fréquents, comme le rappellent les rapports de l'ANSSI et les statistiques de la CNIL sur les incidents liés aux identifiants.

Par ailleurs, les dispositifs existants ne mettent pas en œuvre de verrouillage temporaire après plusieurs tentatives d'identification échouées, ni d'envoi d'alerte à l'administrateur système. Ce type de fonction pourtant basique intégrée dans de nombreuses applications en ligne est ici absent. **Cela traduit un manque de supervision dynamique**, et plus largement une absence d'approche "security by design" dans la conception du module d'accès.

Au-delà de ces failles ponctuelles, les entretiens ont également révélé que les SAE audités reposent parfois sur des composants logiciels anciens, peu maintenus ou issus de bibliothèques open source dont l'évolutivité n'est pas garantie. Ce point renforce le risque d'obsolescence

technique évoqué en Partie I : **une dépendance à des briques logicielles peu robustes peut devenir un vecteur de vulnérabilité**, notamment en cas d'exploitation de failles non corrigées. Comme l'a rappelé un participant, l'absence d'une veille active et d'un plan de mise à jour régulier sur les composants critiques peut transformer une architecture pourtant conforme en "passoire logicielle".

Enfin, même les SAE qualifiés ne sont pas exempts de critiques. Leur certification s'appuie sur une conformité à un moment donné, à travers un audit formel. Mais cette qualification ne garantit ni la surveillance continue, ni la résilience face à des attaques non anticipées. Des résultats de nos observations (avec les informaticiens) il ressort que **la conformité ne doit pas être confondue avec la sécurité réelle**, et le modèle actuel semble davantage axé sur le respect réglementaire que sur la réactivité face à des menaces nouvelles.

En somme, **les dispositifs existants assurent une sécurité structurée, mais peu adaptative**. Ce qui manque, ce n'est pas tant l'implémentation des normes, que la capacité à anticiper et à réagir face aux comportements anormaux, à intégrer une logique de supervision automatisée, et à protéger le système dans son ensemble, au-delà du seul périmètre documentaire. À l'ère des cyberattaques polymorphes et persistantes, cela constitue une faiblesse structurelle préoccupante.

4.3 Analyse des politiques de sauvegarde, de redondance et de récupération après sinistre

Les dispositifs de sauvegarde, de redondance et de reprise après sinistre intégrés aux systèmes d'archivage électronique (SAE) sont traditionnellement perçus comme des garanties de continuité d'accès à l'information. En théorie, leur mission est claire : préserver l'intégrité et la disponibilité des archives, même en cas de sinistre majeur, de cyberattaque ou de défaillance technique. Or, à la lumière de notre étude terrain, il apparaît que ces mécanismes, bien que largement répandus, demeurent insuffisamment adaptés aux menaces évolutives actuelles.

Les entretiens réalisés montrent que la redondance est souvent assurée par des duplications sur plusieurs sites distants ou virtualisés, avec des sauvegardes régulières généralement quotidiennes. Ces mesures correspondent aux bonnes pratiques documentées dans la littérature et offrent une résilience certaine face aux défaillances techniques ordinaires. Toutefois, comme l'illustre de manière frappante l'incident survenu à l'agglomération du Grand Cognac, ces mécanismes montrent leurs limites face à des cyberattaques ciblées. Malgré une infrastructure

multiserveurs, les attaquants ont réussi à compromettre à la fois les serveurs principaux et ceux dédiés aux sauvegardes. Résultat : près d'une décennie d'archives inaccessibles, obligeant l'institution à lancer une campagne de reconstitution des données auprès de ses partenaires.

Ce cas concret remet en cause l'efficacité réelle des dispositifs de redondance lorsqu'ils ne sont pas pensés dans une logique de séparation de zones de confiance. En effet, si les environnements primaire et secondaire partagent des vulnérabilités ou des accès d'administration communs, leur duplication ne fait que propager le risque. Les malwares récents sont d'ailleurs conçus pour détecter et chiffrer les fichiers de sauvegarde, rendant inopérantes les restaurations classiques.

Une autre limite préoccupante est l'absence généralisée de tests systématiques de restauration. Aucun des interlocuteurs consultés ne mentionne l'existence de simulations régulières ou de vérifications formelles de la validité des backups (sauvegardes). Pourtant, comme le rappelle l'ANSSI dans son guide de gestion de crise [41], une politique de continuité n'est pertinente que si elle est éprouvée en condition réelle. Sans test, la restauration devient un pari incertain, dont l'échec au moment critique peut aggraver les dommages initiaux.

Par ailleurs, l'analyse révèle une lacune majeure en matière de journalisation des accès système. Actuellement, la journalisation se limite aux actions effectuées sur les documents eux-mêmes (versement, modification, suppression, etc), sans couvrir les tentatives d'accès ou les échecs de connexion. Or, dans une logique de défense avancée, toute tentative de connexion même infructueuse devrait être consignée, horodatée et signalée. Cette absence de journalisation constitue une vulnérabilité évidente : elle empêche de repérer des tentatives de brute force ou des attaques ciblées sur les comptes à privilèges. Ce constat est renforcé par l'absence de mécanismes de verrouillage automatique après plusieurs tentatives de connexion échouées, observées notamment dans certaines solutions open source analysées (Maarch RM, ICA atom). Aucun système de décompte ou d'alerte automatique à l'intention de l'administrateur n'a été identifié. Pourtant, les standards de sécurité recommandent ce type de dispositif pour prévenir les compromissions de comptes à haut niveau d'autorisation.

Un autre point critique concerne l'accès des administrateurs systèmes. Aujourd'hui, dans la majorité des cas étudiés, les comptes administrateurs disposent de droits étendus, y compris sur le contenu documentaire. En d'autres termes, les administrateurs techniques peuvent accéder à l'ensemble des documents, quels qu'en soient le niveau de confidentialité ou la sensibilité. Ce

constat révèle une confusion persistante entre administration technique du système et gestion des habilitations documentaires. Or, selon les principes du modèle Zero Trust, aucune fonction même technique ne devrait justifier un accès illimité non justifié. Ce modèle, fondé sur la segmentation du réseau et l'authentification continue, impose théoriquement que les administrateurs soient isolés des contenus documentaires sensibles, sauf exception formellement tracée et justifiée. Les normes internationales d'archivage stipulent également que seules les personnes autorisées doivent accéder à des données. Les administrateurs se dérogent à ce jour à cette règle.

Dans une architecture de SAE conforme à cette logique, on attendrait la mise en place de segments distincts : un segment utilisateur (accès contrôlé aux documents selon les profils), un segment d'administration (restreint aux tâches de paramétrage), et un segment de sauvegarde (isolé et inaccessible en exploitation). En l'état actuel, cette séparation n'est que partiellement mise en œuvre, et les administrateurs techniques demeurent des "super utilisateurs" ayant accès à l'ensemble du fonds, ce qui représente une faille éthique autant que sécuritaire.

En somme, si les politiques de sauvegarde et de redondance offrent une couverture satisfaisante contre les incidents techniques courants, elles peinent à répondre aux exigences contemporaines de cybersécurité. L'absence de tests de restauration, la non-journalisation des accès, le manque d'alertes en cas de tentatives suspectes, et l'omnipotence des administrateurs système compromettent la résilience globale des SAE. Face à ces constats, la mise en œuvre du modèle Zero Trust, la redéfinition des droits d'administration, et l'audit régulier des mécanismes de sauvegarde apparaissent comme des leviers indispensables pour renforcer la cybersécurisation des archives numériques

4.4 Problèmes d'interopérabilité et de continuité d'exploitation

Dans un écosystème numérique marqué par l'hétérogénéité croissante des outils et la complexité des infrastructures, les systèmes d'archivage électronique (SAE) sont confrontés à des défis importants d'interopérabilité et de continuité d'exploitation. Ces deux dimensions, souvent abordées de manière technique, relèvent en réalité de véritables enjeux stratégiques : elles conditionnent la capacité des SAE à s'intégrer dans leur environnement, à évoluer avec lui, et à garantir un accès pérenne aux archives numériques.

Les constats issus du terrain révèlent que l'interopérabilité demeure l'un des talons d'Achille des solutions déployées. De nombreux SAE, qu'ils soient open source ou propriétaires, peinent encore à dialoguer efficacement avec les autres systèmes d'information (applications métier, gestion documentaire, messagerie, bases de données). Cette faiblesse résulte notamment de la dépendance persistante à des formats propriétaires (comme .msg, .docx, ou .xls), dont la lisibilité à long terme est sujette à obsolescence ou à des restrictions de compatibilité. Ces formats, bien qu'encore très utilisés, ne garantissent ni la portabilité des contenus, ni leur fidélité sémantique lors des transferts inter-systèmes. L'archiviste est donc contraint de jouer l'intermédiaire entre le SAE et les autres logiciels du système en veillant à convertir les données dans des formats adaptés. Ces limites technologiques ne sont pas sans conséquences en matière de **cybersécurité**, car elles exposent les systèmes aux vulnérabilités des logiciels de conversion et aux failles dans les firmware des scanners. Un scanner dont le firmware n'est pas mis à jour régulièrement peut présenter des vulnérabilités exploitables par des cyberattaquants. Ces failles peuvent permettre une prise de contrôle du périphérique, entraînant l'utilisation du scanner comme point d'entrée pour compromettre le réseau interne.

Ce cloisonnement informationnel s'explique aussi par l'architecture monolithique de certains SAE, qui ne disposent pas de connecteurs d'intégration souples ni de documentation standardisée pour faciliter leur couplage avec d'autres briques applicatives. Or, dans la réalité observée, les SAE sont rarement des outils isolés. Ils doivent interagir avec des chaînes de traitement documentaire, des outils de signature électronique, des solutions de GED ou encore des plateformes de dépôt légal. À défaut de cette interopérabilité, les documents archivés risquent d'être piégés dans des silos, inaccessibles aux autres systèmes, et donc inefficacement conservés.

Le recours au **SEDA** (Standard d'Échange de Données pour l'Archivage) est censé répondre à cette problématique, en normalisant la structure des paquets d'archives (contenu, métadonnées, règles de gestion). Toutefois, d'après les informaticiens consultés, sa mise en œuvre reste techniquement complexe et peu maîtrisée en interne. Sa courbe d'apprentissage et les outils requis pour sa bonne exploitation constituent des obstacles importants pour des structures qui ne disposent ni de ressources spécialisées ni de budget dédié à l'interopérabilité archivistique.

À cette difficulté d'intégration s'ajoute la problématique de la **continuité d'exploitation**. Dans plusieurs cas observés, les SAE sont déployés sans véritable plan de maintenance évolutive, ni

stratégie de mise à jour à moyen terme. Les dépendances à des composants techniques peu maintenus, ou à des prestataires uniques (en cas de solutions propriétaires), accentuent le risque de rupture de service. Le phénomène de **verrouillage technologique** (vendor lock-in) est régulièrement évoqué comme une source d'inquiétude : il limite la capacité de migration, entrave la réversibilité, et met en péril l'accessibilité future des archives en cas d'arrêt de support. Ce manque d'agilité s'observe aussi lors de changements d'environnement (nouveau système d'exploitation, évolution des bases de données, restructuration du réseau). Les SAE ne sont pas toujours conçues pour absorber ces évolutions sans reconfiguration lourde. Pire, l'absence de modularité technique ou de schéma d'intégration clair avec les autres composants du système d'information peut rendre l'adaptation impossible sans refonte partielle, voire totale, de l'outil.

En définitive, les problèmes d'interopérabilité et de continuité d'exploitation soulignent les limites d'une approche trop fermée, trop rigide ou trop dépendante des fournisseurs. Pour garantir la pérennité des archives numériques, il est essentiel d'inscrire les SAE dans une **architecture ouverte, modulaire et interopérable**, fondée sur des standards reconnus, des protocoles d'intégration clairs et une gouvernance documentaire cohérente. Cela implique une **veille technologique permanente**, une **politique de maintenance active**, et surtout une vision systémique du rôle du SAE au sein de l'ensemble informationnel.

4.5 Lacunes en matière d'agilité et d'adaptation face aux menaces dynamiques

Dans un environnement numérique en constante mutation, la capacité des systèmes d'archivage électronique (SAE) à évoluer rapidement pour faire face à de nouvelles menaces constitue un enjeu stratégique majeur. Pourtant, les observations menées révèlent une certaine inertie dans les pratiques actuelles, tant sur le plan technique qu'organisationnel. Les dispositifs en place, bien que efficaces dans des contextes de gestion documentaire classique, montrent de réelles limites dès lors qu'ils sont confrontés à des cybermenaces dynamiques, sophistiquées et imprévisibles.

Les systèmes d'archivage électronique (SAE) sont conçus pour garantir la **fiabilité**, la **traçabilité** et le **respect des réglementations**. Cela signifie qu'ils doivent conserver des documents en l'état, sans modification imprévue, afin de préserver leur valeur légale et historique. Cependant, cette approche rend ces systèmes **rigides**, et donc **difficiles à adapter** en cas de menace informatique. Lorsqu'un problème de sécurité survient comme une faille

logicielle ou une attaque malveillante, il est contraignant d'appliquer des correctifs rapidement. Chaque mise à jour ou modification technique peut poser un **risque** pour l'intégrité des documents archivés, et nécessite donc des précautions supplémentaires. Ainsi, les corrections peuvent être retardées ou appliquées manuellement, ce qui laisse des **failles temporaires** où des cyberattaques peuvent se produire.

Il convient également de rappeler que certains SAE pourraient nécessiter une revalidation ou une homologation complète à chaque mise à jour majeure, notamment lorsqu'ils sont associés à des processus d'archivage probatoire. Si cette exigence vise à garantir la conformité, elle bloque cependant toute forme d'agilité face à des attaques évolutives, en contradiction avec le rythme imposé par les cybermenaces actuelles. Cette rigidité n'est pas uniquement imputable à l'outil. Elle trouve également ses racines dans l'organisation elle-même. Dans plusieurs structures observées, la gestion de la sécurité des archives reste fragmentée entre les équipes techniques, les archivistes, les juristes et les responsables métier. Il en résulte une absence de pilotage transversal, de cellules de veille active, ou de dispositifs de retour d'expérience structurés après incident. Sans coordination centralisée, la gestion du risque cyber devient réactive, et non anticipative. Or, dans un contexte où les attaques ciblées peuvent évoluer en quelques heures, seule une approche prédictive peut garantir la protection effective des archives. Cela suppose d'introduire des mécanismes plus évolués d'analyse comportementale, de détection d'anomalies, ou de réaction automatisée à l'intrusion. Ces technologies ne sont encore que très marginalement intégrées dans les SAE étudiés, dont les capacités de veille interne sont souvent absentes ou minimalistes.

Parmi les solutions envisagées, le modèle **Zero Trust** apparaît comme une piste sérieuse. Ce modèle repose sur une présomption de non-fiabilité permanente. Chaque accès, chaque requête, chaque interaction est vérifiée systématiquement, même si elle émane de l'intérieur du système. Appliqué aux SAE, il permettrait d'introduire une logique d'isolement, de limitation des mouvements latéraux, et de segmentation fine des droits d'accès en particulier pour les administrateurs systèmes, qui conservent aujourd'hui un accès complet à l'ensemble des contenus, y compris ceux auxquels ils ne devraient pas avoir de visibilité. Cette situation, encore largement tolérée dans de nombreux environnements, constitue une faille structurelle grave. Le fait que les administrateurs disposent d'un pouvoir technique total sur les contenus, en contradiction avec les principes d'habilitation, met en péril la confidentialité des archives sensibles et crée un risque interne important. Enfin, l'absence généralisée d'outils de

surveillance active ou de cyberveille spécifique aux SAE limite leur capacité à réagir en temps réel. Dans un environnement où l'automatisation de l'attaque est désormais courante, l'automatisation de la défense devient incontournable.

En somme, la posture actuelle des SAE face aux menaces dynamiques reste trop figée. Le socle normatif et les mécanismes traditionnels (journalisation, contrôle d'accès, redondance) apportent une protection structurante, mais pas suffisante. Face à la sophistication des attaques, les dispositifs doivent évoluer vers une cybersécurité vivante, portée par une culture du risque et des technologies adaptatives. Ce constat général, qui clôt la série d'analyses critiques portant sur les dispositifs existants, ouvre naturellement sur la nécessité d'un renouvellement des approches techniques et stratégiques. Le chapitre suivant se consacrera ainsi à l'exploration des technologies émergentes susceptibles de renforcer la résilience des SAE et de mieux les armer face aux défis de demain.

Chapitre 5 - Innovations et solutions émergentes pour renforcer la cybersécurité des SAE

Alors que les dispositifs classiques de sécurité des systèmes d'archivage électronique (SAE) montrent leurs limites face à l'accélération des menaces numériques, l'attention se porte désormais sur les **innovations technologiques susceptibles de renouveler les approches de cybersécurisation**. Ces avancées récentes issues tant du champ de la cryptographie que de l'intelligence artificielle ou de la gouvernance numérique offrent des perspectives prometteuses, mais encore largement en phase d'expérimentation ou de normalisation. Ce mouvement soulève une interrogation centrale : ces technologies émergentes peuvent-elles réellement apporter des garanties supplémentaires en matière de fiabilité, de résilience et de confiance pour l'archivage numérique ? Ce chapitre propose d'examiner successivement les apports potentiels de la blockchain pour l'archivage probatoire, le rôle des portefeuilles numériques dans la gestion d'identité et le partage sécurisé, l'intégration de l'IA dans la cybersécurité prédictive, ainsi que les effets attendus des nouveaux standards européens de certification.

5.1 Blockchain et archivage à valeur probatoire

La blockchain est une technologie reposant sur un ensemble de protocoles et de règles pour créer un réseau de stockage et de transmission de données sécurisé et décentralisé. En gros, la blockchain est une base de données distribuée, où chaque participant du réseau joue un rôle

dans la validation et l'enregistrement des transactions [42]. La blockchain suscite un vif engouement dans le secteur de l'archivage électronique, notamment pour ses promesses en matière de traçabilité, d'inaltérabilité et de certification décentralisée. À première vue, cette technologie semble répondre à plusieurs fragilités des SAE traditionnels comme la centralisation excessive des preuves, la dépendance à un prestataire unique, ou l'altérabilité des journaux internes. Elle se positionne comme une alternative crédible pour sécuriser les archives à haute valeur probatoire. Mais les observations issues du terrain et les retours de professionnels en cybersécurité appellent à tempérer cet enthousiasme.

En pratique, aucun des systèmes observés n'intègre aujourd'hui de manière native une couche blockchain. Les solutions existantes restent centrées sur des mécanismes de traçabilité internes, certes conformes aux normes (comme la NF Z42-013), mais encore vulnérables à des altérations en cas de compromission de l'environnement. C'est dans ce contexte que la blockchain apparaît comme un outil d'ancrage externe, permettant de générer une preuve indépendante de la plateforme elle-même.

Cependant, plusieurs limites techniques freinent son adoption à court terme. D'abord, l'intégration d'une chaîne de blocs exige une infrastructure distribuée, une gouvernance partagée, et des compétences cryptographiques avancées que peu d'organisations maîtrisent actuellement. Les éditeurs de SAE, notamment open source, ne proposent pas encore de modules blockchain prêts à l'emploi, ce qui rend l'implémentation dépendante de développements spécifiques, lourds à maintenir.

Ensuite, la blockchain garantit l'intégrité d'une empreinte numérique, mais non du document lui-même. Elle ne protège ni contre la fraude initiale (création d'un faux document « propre »), ni contre les erreurs de gestion documentaire en amont. Elle ne résout donc qu'une partie du problème sécuritaire : celui de l'inaltérabilité après dépôt, mais pas celui de la fiabilité de la chaîne documentaire complète.

À cela s'ajoutent des interrogations sérieuses sur la souveraineté des données. L'utilisation de blockchains publiques pose des risques de gouvernance, de localisation des nœuds, et de conformité réglementaire (notamment RGPD ou exigences de territorialité). Il faut aussi souligner que la blockchain n'est pas une réponse adaptée à tous les types d'archives. Son usage se justifie principalement pour des documents sensibles, à forte valeur de preuve : contrats,

décisions juridiques, identités numériques. Pour des volumes d'archives courantes ou à faible criticité, son déploiement apparaît surdimensionné, voire inutilement complexe.

Les expérimentations actuelles (notamment avec des coffres-forts numériques adossés à la blockchain) sont intéressantes mais encore accesseoires. Elles démontrent une faisabilité technique, mais pas nécessairement une viabilité économique ou opérationnelle à grande échelle. En réalité, ces projets restent souvent portés par des logiques d'innovation ou de communication, plus que par une réelle demande fonctionnelle du terrain.

En définitive, la blockchain constitue une avancée technologique pertinente dans certains cas d'usage, mais ne peut être considérée comme une solution globale ou immédiate à la sécurisation des SAE. Son intégration suppose une stratégie claire, une maîtrise technique forte, et un alignement avec les exigences archivistiques et juridiques. À ce jour, elle relève encore davantage du champ des perspectives que de celui des solutions pleinement opérationnelles.

5.2 Wallets numériques : une piste prometteuse pour la gestion d'identité et le partage sécurisé dans les SAE

À mesure que les exigences en matière de cybersécurité se renforcent dans les environnements documentaires, la question de **l'authentification forte et du partage sécurisé des archives** devient centrale. Dans ce contexte, l'émergence des wallets numériques ou portefeuilles numériques d'identité ouvre des perspectives intéressantes, bien que leur usage ne soit, à ce jour, **pas encore orienté vers les systèmes d'archivage électronique**. C'est donc moins un retour d'expérience qu'une **analyse prospective** qui s'impose ici.

Les wallets numériques, tels que ceux développés dans le cadre du projet européen **EUDI Wallet**, permettent à un individu de **gérer lui-même ses données d'identité, ses certificats et ses autorisations d'accès**, dans une logique de sécurité décentralisée. Ils sont aujourd'hui testés dans des domaines comme la finance, les services publics ou les procédures administratives. Leur extension potentielle au domaine de l'archivage repose sur une intuition forte : **assurer une traçabilité et une non-répudiation renforcées dans les opérations d'accès, de partage ou de consultation des archives sensibles**. À la différence des systèmes classiques d'habilitation, souvent fondés sur des rôles internes rigides, les wallets permettent une **gestion dynamique, granulaire et vérifiable des identités**. Chaque action documentaire pourrait ainsi être conditionnée par l'identité certifiée du porteur, sa localisation, ou son niveau d'habilitation,

tous contenus dans le wallet. En ce sens, ces outils offriraient un véritable levier pour renforcer les principes de confidentialité, d'**authentification à deux facteurs**, et de **contrôle contextuel des accès**.

Avec une mise en œuvre prévue dans l'espace de l'Union Européenne d'ici fin 2026, « le système EUDI Wallet offrira de multiples fonctionnalités, notamment l'authentification sécurisée, le stockage de documents, les capacités de partage et la signature numérique. Les citoyens pourront stocker et gérer divers justificatifs d'identité, y compris des données d'identification personnelle, des diplômes universitaires et des permis de conduire, en utilisant ces portefeuilles pour accéder aux services du gouvernement et du secteur privé » [43].

Néanmoins des enjeux critiques subsistent. La **souveraineté numérique** reste un point de vigilance : qui contrôle l'infrastructure du wallet ? Où sont stockées les clés ? Quelles sont les garanties en cas de compromission du terminal ou d'usurpation d'identité ? Sans des **coffres-forts, des protocoles stricts d'authentification** et une **gestion rigoureuse des consentements**, ces solutions pourraient devenir des points de vulnérabilité plutôt que de confiance. Le projet prévoit déjà un cadre fonctionnel ambitieux. Selon la Commission européenne, « l'Agence de l'Union européenne pour la cybersécurité (ENISA) a été chargée d'élaborer des systèmes complets de certification de cybersécurité afin de garantir la sécurité et la fiabilité de ces portefeuilles » [43]. Toutefois, au regard de la recrudescence des cyberattaques visant même les géants du numérique, il convient de rappeler que les autorités de confiance ne sont pas elles-mêmes à l'abri.

Par ailleurs, leur adoption nécessiterait une refonte profonde des modèles d'habilitation des SAE, encore largement fondés sur une administration centralisée. Elle supposerait également une interopérabilité stricte avec les normes d'identification électronique reconnues (eIDAS), et un accompagnement juridique sur la valeur probante des accès validés via wallet.

En définitive**,** les wallets numériques ne représentent pas aujourd'hui une solution à intégrer aux SAE, mais ils pourraient représenter une évolution naturelle pour répondre aux nouveaux défis de l'accès sécurisé, de l'imputabilité, et du partage contrôlé des archives sensibles. Leur apport potentiel réside moins dans la conservation des documents que dans la gestion sécurisée de leur circulation. Encore faut-il que les éditeurs de SAE, les autorités de régulation et les professionnels de l'archivage s'approprient ces outils, dans une logique d'adaptation des pratiques, de montée en compétence, et de renouvellement des référentiels de sécurité.

5.3 Intelligence artificielle et cybersécurité prédictive : un déséquilibre entre acteurs défensifs et pirates

L'un des paradoxes majeurs de la cybersécurité contemporaine réside dans le fait que l'intelligence artificielle (IA) est aujourd'hui mobilisée des deux côtés du front : par les acteurs défensifs comme par les cyberattaquants. Génération automatisée de malwares, deepfakes documentaires, détection de failles en temps réel, campagnes de phishing personnalisées, les outils offensifs exploitent déjà l'IA avec une agilité croissante. Dès lors, envisager l'IA comme rempart dans les systèmes d'archivage électronique (SAE) revient à engager une confrontation symétrique entre deux puissances algorithmiques. Ce n'est pas l'outil qui crée l'avantage stratégique, mais le niveau de maîtrise des acteurs qui le manipulent.

Or, de ce point de vue, le déséquilibre est manifeste. Les cyberattaquants se forment, expérimentent, itèrent à un rythme soutenu, souvent en dehors de tout cadre réglementaire. À l'inverse, les milieux professionnels de l'information et notamment les archivistes restent encore largement en marge de ces dynamiques. L'IA n'est que marginalement abordée dans les formations initiales en archivistique, et la cybersécurité, quand elle est évoquée, reste cantonnée à des techniques réservées aux administrateurs ou aux RSSI. Il n'existe à ce jour ni culture partagée, ni exigence formalisée de compétences en IA dans les métiers de l'archivage, alors même que ces derniers manipulent des données critiques quotidiennement. Ce retard d'acculturation devient problématique à l'heure où les solutions de sécurité intégrées aux SAE commencent à se reposer sur des dispositifs automatisés de détection, de journalisation ou de surveillance comportementale. Il est illusoire de déléguer l'intégralité de la vigilance aux seuls informaticiens, comme il serait irresponsable de faire de l'IA une simple boîte noire supposée "protéger par défaut". La maîtrise des outils défensifs doit être partagée. Les professionnels de l'information doivent comprendre les mécanismes, les biais possibles, les seuils de déclenchement, et les limites des algorithmes qu'ils utilisent.

La montée en puissance de l'IA dans la cybersécurité documentaire impose une refonte urgente des pratiques pédagogiques, mais aussi des stratégies organisationnelles. Il ne s'agit pas simplement d'initier les agents aux bons réflexes numériques, mais de leur apprendre à dialoguer avec les machines, à formuler des requêtes intelligentes, à interpréter des signaux faibles, et à prendre des décisions informées face à des alertes générées automatiquement. Le prompt engineering doit devenir une compétence de base, au même titre que la maîtrise des

métadonnées ou la compréhension des normes d'archivage. Dans cette configuration, l'IA défensive ne peut être efficace que si elle est soutenue par une montée en compétences globale, transversale, et non discriminante. Restreindre l'usage de ces technologies aux seuls profils techniques revient à fragiliser l'ensemble de la chaîne documentaire. La cybersécurité ne doit plus être un domaine réservé ; elle doit devenir une responsabilité partagée, intégrée aux gestes quotidiens, à la culture professionnelle et aux plans de formation.

En définitive, l'intégration de l'intelligence artificielle dans les SAE n'est ni une panacée, ni une simple évolution technique. C'est une mutation structurelle qui oblige les institutions à repenser la place du savoir, la circulation des compétences, et la capacité collective à affronter un environnement menaçant. Tant que les professionnels de l'information resteront à distance de ces outils, les systèmes qu'ils gèrent seront vulnérables non pas par faiblesse technique, mais par défaut de gouvernance et d'anticipation stratégique.

5.4 Standards européens et certification de confiance : une excellence à étendre, mais à rééquilibrer

L'encadrement normatif des systèmes d'archivage électronique a franchi un seuil qualitatif important avec le règlement eIDAS et son extension en 2024 par le règlement (UE) 2024/1183. Ces dispositifs constituent aujourd'hui une référence rigoureuse, en matière de valeur probatoire, de sécurité des échanges, et de certification des prestataires de services de confiance. Leur niveau d'exigence et leur cohérence technique offrent un socle d'excellence, dont l'extension à l'échelle internationale pourrait renforcer l'universalité des bonnes pratiques archivistiques en matière de cybersécurité.

En effet, si les normes ISO archivistiques assurent déjà des garanties sur l'intégrité documentaire (comme ISO 14721 ou ISO 16175), elles restent peu prescriptives sur la **gestion sécuritaire en temps réel** : la veille des vulnérabilités, la supervision des accès sensibles ou la résilience technique sont encore des angles morts normatifs. Pour les pays à faible couverture réglementaire, une convergence entre les standards ISO et les exigences européennes pourrait constituer un levier stratégique majeur pour garantir un **niveau de sécurité de base** à l'échelle mondiale, tout en diffusant les modèles européens de gouvernance documentaire sécurisée.

Néanmoins, cette ambition mérite d'être nuancée par une série de **contradictions structurelles** du modèle actuel. Si les standards européens promeuvent la rigueur, ils induisent aussi une

concentration croissante de la confiance autour d'un nombre restreint de prestataires qualifiés. En centralisant l'autorité sur des organismes labellisés, le risque devient systémique. Le moindre incident sur un de ces prestataires pourrait affecter l'intégrité globale des dispositifs de confiance. Or, comme tout acteur numérique, ces prestataires restent vulnérables aux erreurs internes, aux dépendances logicielles critiques, ou à des attaques ciblées.

À cela s'ajoute un défaut structurel du modèle actuel. La certification garantit une conformité à un instant donné, mais n'assure ni la mise à jour continue**,** ni l'adaptabilité du système face à l'émergence de nouvelles menaces. Appliquer un correctif de sécurité critique, modifier un paramètre de configuration ou intégrer un nouveau protocole peut exiger une réévaluation complète du système, ce qui **freine parfois les initiatives proactives**. Ce paradoxe un SAE conforme mais vulnérable est d'autant plus préoccupant qu'il repose sur une interprétation statique de la cybersécurité, alors même que celle-ci est, par nature, évolutive.

Cependant des solutions commencent à se révéler, notamment du côté de l'ANSSI, pour proposer une **certification dynamique** reposant sur des contrôles réguliers, des tests de pénétration programmés, une surveillance comportementale et des indicateurs de résilience documentés. Cette approche viserait non plus seulement à constater la conformité, mais à **piloter la sécurité dans la durée**, en intégrant les principes de supervision active et de transparence opérationnelle.

Par ailleurs, **il serait risqué de fonder l'ensemble de la cybersécurité des archives numériques sur une seule typologie d'acteurs**. La légitimité des prestataires de confiance ne doit pas se transformer en exclusivité de confiance. Une approche équilibrée supposerait de croiser leurs mécanismes de validation avec d'autres outils (ex. : vérification interne, co-sécurisation par plusieurs autorités, technologies disruptives comme la blockchain), dans une logique de **sécurité redondante** et **décentralisée**. Comme pour l'authentification à deux facteurs, c'est dans **la pluralité des couches de protection** que réside la robustesse.

Retenons sur ces notes que les standards européens constituent une base normative précieuse, qu'il serait pertinent d'**étendre aux référentiels archivistiques internationaux**, afin de créer un socle commun de cybersécurité documentaire. Mais cette extension ne saurait faire l'économie d'une **révision profonde du paradigme de certification** : plus dynamique, plus ouvert, plus distribué. La sécurité documentaire ne peut reposer exclusivement sur la conformité réglementaire ; elle doit s'ancrer dans une gouvernance partagée, dans la capacité d'évolution,

et dans une vigilance continue à l'égard des vulnérabilités systémiques, y compris chez ceux qui incarnent aujourd'hui la confiance.

En définitive, si les innovations technologiques, les mécanismes prédictifs et les standards européens apportent des avancées notables en matière de cybersécurité des systèmes d'archivage électronique, ils ne suffisent pas, à eux seuls, à garantir une protection durable. La complexité des menaces actuelles impose une approche plus fondée sur la complémentarité des outils, la diversification des acteurs, et une gouvernance souple mais rigoureuse. Dès lors, il devient essentiel de penser au-delà des solutions existantes, pour dégager des **recommandations stratégiques et opérationnelles** capables d'assurer une sécurisation à la fois évolutive, réaliste et adaptée aux enjeux de demain ce que nous aborderons dans le chapitre suivant.

Chapitre 6 - Recommandations pour une stratégie de résilience des SAE

À l'issue des constats théoriques et critiques établis dans les précédents chapitres, il apparaît que la sécurité des systèmes d'archivage électronique (SAE) ne peut plus reposer uniquement sur des dispositifs techniques ou sur la conformité à des normes. Elle doit désormais s'inscrire dans une approche plus globale, orientée vers la résilience, c'est-à-dire la capacité du système à résister, s'adapter et se réorganiser face à des perturbations imprévues. Dès lors, une question essentielle se pose : quels leviers stratégiques, organisationnels et humains les organisations peuvent-elles mobiliser pour construire une SAE à la fois robuste, évolutif et pérenne ? Ce dernier chapitre propose une série de recommandations concrètes, articulées autour de quatre axes : l'intégration de la sécurité dès la conception des systèmes, le renforcement des audits et de la gestion des vulnérabilités, la sensibilisation des acteurs de l'archivage, et la mise en place d'un modèle de gouvernance adaptatif et collaboratif.

6.1 Intégration des principes de cybersécurité dès la conception du SAE

Une stratégie de résilience réellement efficace pour les systèmes d'archivage électronique (SAE) doit impérativement commencer dès leur phase de conception. Trop souvent, les dispositifs de sécurité sont pensés après coup, comme des modules que l'on ajoute une fois que le système est en place, créant ainsi des failles structurelles difficiles à corriger. Or, dans un environnement numérique où les menaces évoluent plus rapidement que les dispositifs de protection, cette logique atteint rapidement ses limites. La sécurité ne peut pas être un

supplément technique ; elle doit faire partie de l'ADN du SAE dès les premiers schémas de conception.

Intégrer la cybersécurité dès le départ, c'est adopter une logique dite de "security by design" ou de "sécurité par la conception". Cela signifie que dès la phase de modélisation fonctionnelle, chaque brique du système qu'il s'agisse de la gestion des identités, de l'attribution des droits, de la traçabilité des actions, du chiffrement des données, ou de la surveillance des comportements doit être pensée avec des objectifs clairs de sécurité [43]. Ces mesures doivent être calibrées en fonction de la sensibilité des documents archivés, de leur durée de conservation et des obligations réglementaires auxquelles ils sont soumis. Il s'agit non seulement de prévenir les intrusions, mais aussi d'anticiper les usages déviants, de garantir la continuité d'accès légitime, et de documenter toute action significative dans un journal infalsifiable.

Ce type d'intégration suppose une collaboration active entre plusieurs métiers : les informaticiens, les architectes de solutions, les experts en cybersécurité, mais aussi les archivistes et les juristes. Ces derniers ne doivent pas être de simples observateurs ou utilisateurs finaux : ils doivent pouvoir intervenir dès la définition des scénarios d'usage, participer à la validation des risques et exprimer des exigences précises, notamment en matière de traçabilité, de conservation probatoire ou d'accès différencié aux documents. Trop souvent encore, les décisions techniques sont prises en vase clos, sans prise en compte suffisante des exigences documentaires, ce qui nuit à la cohérence globale du système.

Un autre enjeu majeur réside dans la capacité à anticiper les zones d'ombre fonctionnelles. Il ne suffit pas de tracer les actions critiques comme les suppressions de documents : il faut aussi s'intéresser à des événements plus subtils, comme les tentatives d'accès à des interfaces sensibles ou les consultations récurrentes de certains contenus par des profils inattendus. Ces signaux faibles, souvent révélateurs d'un comportement suspect, doivent être non seulement captés, mais analysés et mis en perspective dans une logique de prévention active.

Enfin, intégrer la cybersécurité dès la conception permet de mieux gérer l'évolution du système dans le temps. En prévoyant des interfaces modulaires, des dispositifs de journalisation extensibles ou des mécanismes d'authentification adaptatifs, on prépare le SAE à s'adapter aux évolutions technologiques et réglementaires sans nécessiter de refonte lourde ou risquée. Cela réduit les coûts, améliore la sécurité, et renforce la confiance des utilisateurs comme des autorités de contrôle.

Ainsi, une véritable démarche de "security by design" ne se résume pas à cocher des cases dans un référentiel. Elle constitue une posture proactive, transversale, et collaborative, qui transforme la sécurité en levier d'optimisation globale du SAE. En intégrant ces principes dès les premières lignes du cahier des charges, les organisations s'offrent une meilleure maîtrise des risques, une conformité durable et une robustesse accrue face aux défis de la cybersécurité contemporaine.

6.2 Renforcement des audits de sécurité et de la gestion des vulnérabilités

Le renforcement des audits de sécurité, couplé à une gestion active et continue des vulnérabilités, représente aujourd'hui une réponse stratégique incontournable. Il ne s'agit plus seulement d'appliquer des normes pour se conformer à la réglementation, mais de mettre en place une véritable culture de la sécurité ancrée dans tous les cycles de vie du SAE. Cela commence par une nouvelle compréhension de l'audit de sécurité, non plus perçu comme une démarche administrative, mais comme un véritable outil de diagnostic stratégique. Un audit permet d'évaluer les capacités réelles du SAE à préserver la confidentialité, l'intégrité, la disponibilité et la traçabilité des archives numériques. Il porte sur la configuration technique, les pratiques organisationnelles, les dispositifs juridiques, et doit être déclenché à chaque évolution majeure du système. Confier cette mission à des acteurs compétents, qu'ils soient internes ou externes, garantit une évaluation impartiale, surtout lorsqu'on s'appuie sur des méthodologies reconnues comme celles de l'ISO 27001, du SecNumCloud ou des guides de l'ANSSI.

Mais l'audit, même bien mené, ne suffit pas. Il donne un état des lieux à un instant donné, alors que les menaces, elles, évoluent en permanence. D'où l'importance de bâtir une véritable politique de gestion des vulnérabilités. Cette politique repose sur la mise en place d'une veille technique constante, pour repérer les failles connues sur les composants du SAE. Elle implique aussi la capacité d'agir rapidement : hiérarchiser les correctifs à appliquer selon leur criticité, planifier les mises à jour et documenter systématiquement chaque intervention. Cette documentation joue un rôle crucial. Elle permet de prouver, à tout moment, que l'on a pris les mesures nécessaires, en cas d'audit externe ou d'enquête post-incident. Dans les environnements les plus matures, cette gestion repose sur des outils automatisés qui scannent les vulnérabilités, proposent des corrections et permettent de suivre la sécurité du système via

des indicateurs clairs. Pour autant, ces outils doivent être interprétés par des professionnels, car leur efficacité dépend de la compréhension fine du contexte.

Il est donc essentiel d'intégrer la gestion des vulnérabilités dès la conception du SAE et de l'inscrire dans toutes ses évolutions. Cela implique, concrètement, de nommer un référent sécurité qui coordonnera les actions correctives, de veiller à ce que chaque mise à jour logicielle intègre des exigences de cybersécurité, et de structurer une gouvernance dans laquelle tous les acteurs concernés, des informaticiens aux archivistes en passant par les prestataires, puissent dialoguer, valider les décisions et répondre rapidement aux incidents. Cette gouvernance partagée permet d'éviter les silos de responsabilité et d'assurer une approche globale de la sécurité.

À cette gestion planifiée et partagée peut s'ajouter une dimension proactive : les tests de pénétration, aussi appelés pentests. Ils consistent à simuler des attaques informatiques pour identifier les faiblesses opérationnelles réelles du système. Ce type de test permet souvent de repérer des failles que l'audit classique ne détecte pas, notamment celles liées aux configurations spécifiques, aux droits d'accès mal calibrés ou aux connexions avec d'autres systèmes. En parallèle, il devient pertinent d'implémenter des dispositifs de supervision continue. Ces dispositifs automatisés surveillent en permanence le bon fonctionnement du SAE, détectent toute anomalie ou écart de conformité, envoient des alertes et génèrent des rapports exploitables pour ajuster rapidement les politiques de sécurité.

En définitive, renforcer les audits de sécurité et organiser une gestion continue des vulnérabilités, ce n'est pas seulement adopter de bonnes pratiques : c'est s'engager sur le long terme pour bâtir des systèmes résilients. C'est aussi reconnaître que la cybersécurité n'est jamais acquise, qu'elle exige des efforts constants, partagés, et documentés. En inscrivant ces dispositifs dans une stratégie claire, en les intégrant à la gouvernance globale des SAE, on passe d'une logique défensive ponctuelle à une culture active de la sécurité, condition sine qua non de la confiance dans la conservation numérique à long terme.

6.3 Sensibilisation, formation et culture de la sécurité pour les archivistes

L'efficacité d'un système d'archivage électronique repose autant sur les technologies mises en œuvre que sur les usages quotidiens qui en sont faits par les professionnels. Parmi ces acteurs, les archivistes occupent une position stratégique, à la fois gestionnaires du patrimoine

documentaire et garants de sa protection sur le long terme. Pourtant, leur rôle dans la sécurité des systèmes est encore trop souvent sous-estimé ou marginalisé. Dans de nombreuses organisations, la cybersécurité est perçue comme un domaine exclusivement technique, réservé aux informaticiens ou aux prestataires externes. Cette segmentation des responsabilités empêche la mise en place d'une culture commune de la sécurité et expose les systèmes à des risques accrus d'erreurs humaines, de négligences ou de malentendus entre métiers.

Pour y remédier, il est essentiel de reconnaître les archivistes comme des acteurs à part entière de la gouvernance de la sécurité numérique. Cela commence par une politique de sensibilisation active, intégrée aux routines de travail. Les archivistes doivent être en mesure d'identifier les menaces les plus fréquentes telles que les tentatives d'hameçonnage, les logiciels malveillants ou les manipulations de métadonnées et d'adopter des réflexes simples mais efficaces : signalement des anomalies, application stricte des règles de journalisation, vérification des accès, sécurisation des fichiers. Cette sensibilisation ne doit pas se limiter à des rappels généraux, mais prendre des formes concrètes et récurrentes : ateliers pratiques, simulations d'incidents, diffusion de fiches réflexes ou insertion de rappels dans les réunions de service. Elle doit également être portée par des relais identifiés au sein des services d'archives, en lien avec les experts en sécurité de l'information.

Mais au-delà de la sensibilisation, une véritable montée en compétence est indispensable. Les archivistes doivent bénéficier de formations adaptées, leur permettant de comprendre les bases de la sécurité des systèmes d'information, les référentiels applicables au domaine de l'archivage, les mécanismes d'authentification, de chiffrement, de journalisation et de contrôle d'accès, ainsi que les procédures à suivre en cas d'incident. Ces formations doivent être conçues selon les profils : agents techniques, responsables de service, chefs de projet GED, et inscrites durablement dans les plans de développement des compétences. L'objectif n'est pas de transformer les archivistes en experts en cybersécurité, mais de les rendre capables d'interagir efficacement avec les informaticiens, de faire remonter des alertes pertinentes, de poser les bonnes questions et de défendre les exigences archivistiques en matière de sécurité.

Cette transformation passe aussi par une évolution des représentations institutionnelles. Il est crucial d'associer les professionnels de l'archivage aux instances de gouvernance de la sécurité comités de pilotage, revues de risques, choix d'architecture afin qu'ils puissent contribuer activement aux décisions et défendre les spécificités liées à la conservation des documents.

Cette reconnaissance de leur expertise permet de construire une approche transversale de la cybersécurité, fondée sur la complémentarité des savoirs techniques, juridiques et documentaires. Les retours d'expérience montrent que les structures qui adoptent une telle démarche sont plus résilientes, plus réactives face aux crises, et bénéficient d'un climat de confiance renforcé, tant en interne qu'avec leurs partenaires.

En somme, renforcer la culture de la cybersécurité chez les archivistes, ce n'est pas seulement améliorer la sécurité d'un point de vue technique. C'est initier une transformation organisationnelle profonde, dans laquelle chaque professionnel de l'archivage devient un acteur conscient, compétent et engagé dans la protection durable du patrimoine numérique.

6.4 Vers un modèle de gouvernance adaptative et collaborative

Face à l'instabilité croissante du paysage numérique, à la multiplication des cybermenaces et à la complexité des environnements d'archivage électronique, il devient impératif de repenser la manière dont les organisations pilotent la sécurité de leurs systèmes. Une stratégie de résilience efficace ne peut se limiter à des dispositifs techniques isolés ou à une application rigide de normes : elle doit s'appuyer sur un mode de gouvernance vivant, transversal, et en constante adaptation.

La gouvernance classique des SAE repose souvent sur des schémas descendus, où les décisions sont prises par quelques acteurs direction des systèmes d'information, prestataires externes et communiquées ensuite aux services utilisateurs. Ce modèle vertical peut ralentir les réponses en cas d'incident et engendrer des incompréhensions entre métiers. À l'inverse, une gouvernance adaptative repose sur la coopération entre les différents services concernés (archives, informatique, juridique, conformité) et sur des circuits de décision agiles. Elle permet d'absorber les crises, de réagir rapidement, et de maintenir la disponibilité du SAE même dans un contexte instable.

Mettre en place un tel modèle suppose d'instaurer des instances de dialogue régulières, de produire et partager des indicateurs de sécurité accessibles à tous, et de capitaliser systématiquement sur les retours d'expérience. C'est dans l'échange et la mutualisation que se construit une sécurité efficace. Par exemple, un incident constaté par un archiviste doit pouvoir être remonté sans filtre, analysé collectivement, et déboucher sur des actions concrètes,

partagées avec l'ensemble des acteurs. Il ne s'agit pas de créer une usine à gaz, mais de structurer des réflexes collectifs.

La gouvernance collaborative suppose également de formaliser les responsabilités et les procédures. Un référentiel de gouvernance interne, régulièrement mis à jour, peut ainsi décrire les rôles de chacun, les protocoles à suivre en cas de faille, les échéances des audits, les processus de remontée d'information, etc. Ce document doit être le fruit d'un travail conjoint, nourri par l'expérience des utilisateurs, des techniciens et des responsables de la conformité. Il sert de cadre souple mais clair pour prendre des décisions en situation critique.

Enfin, le dialogue entre les métiers informaticiens, archivistes, juristes est la clé d'une confiance durable dans le SAE. Chacun détient une partie de la connaissance : technique, documentaire, réglementaire. Ce n'est qu'en croisant ces regards que l'on peut bâtir un système à la fois sûr, efficace et adapté aux besoins réels. La gouvernance n'est donc pas un simple organe de contrôle : elle devient un espace de coordination et d'intelligence collective. Dans un monde numérique incertain, cette capacité à collaborer et à s'adapter collectivement constitue l'un des premiers facteurs de résilience d'un système d'archivage électronique.

De tout ce qui précède, nous pouvons conclure que la résilience d'un système d'archivage électronique (SAE) ne s'improvise pas. Elle se construit avec le temps grâce à une architecture bien pensée, des processus de gestion rigoureux, des équipes compétentes et une gouvernance ouverte. En combinant ces éléments, les organisations peuvent faire du SAE un véritable outil de confiance numérique, capable de s'adapter et de garantir la pérennité des archives malgré les évolutions et les défis du numérique.

Les recommandations formulées dans ce chapitre visent à dépasser une logique strictement défensive pour inscrire les systèmes d'archivage électronique dans une stratégie de cybersécurité résolument résiliente. Car malgré l'apparente solidité des cadres normatifs et des architectures techniques déployées, les SAE restent exposées à des menaces multiples : erreurs humaines, obsolescence logicielle, attaques ciblées, défauts de journalisation ou encore insuffisance des mécanismes de reprise d'activité. L'intégration des exigences de sécurité dès la phase de conception, le renforcement des audits et de la gestion proactive des vulnérabilités, la montée en compétence des professionnels de l'archivage et l'adoption d'un modèle de gouvernance adaptatif apparaissent comme les leviers clés d'une protection durable des archives numériques. Ces orientations, fondées sur les constats des chapitres précédents, rappellent que la sécurisation des SAE ne peut être assurée par la technologie seule : elle requiert une approche systémique, fondée sur la collaboration interdisciplinaire, l'anticipation stratégique et la responsabilisation de l'ensemble des parties prenantes.

Conclusion générale

Face à l'essor de la dématérialisation, les systèmes d'archivage électronique (SAE) se sont imposés comme des outils structurants pour garantir la pérennité, la traçabilité et la légitimité des documents numériques. Leur rôle est crucial dans un environnement informationnel de plus en plus exposé aux risques cybernétiques, à la complexité réglementaire, et à l'obsolescence technologique. Pourtant, malgré une base réglementaire robuste et des objectifs fonctionnels clairement établis, ces systèmes ne peuvent être considérés comme infaillibles.

L'analyse menée dans la première partie a permis d'identifier les principes fondamentaux qui sous-tendent la sécurisation des SAE : respect des normes (NF Z42-013, ISO 14641, etc.), traçabilité des actions, garantie d'intégrité et d'authenticité documentaire, cloisonnement des accès et gouvernance des rôles. Ces principes offrent une assise solide en théorie, mais leur application effective dépend de la manière dont les outils sont conçus, développés et intégrés dans les environnements métiers.

Dans la seconde partie, un travail critique basé sur des retours d'expérience et des observations de terrain a permis de mettre en lumière un écart notable entre les cadres de référence existants et les pratiques concrètes des éditeurs de logiciels. Plusieurs vulnérabilités structurelles ont été relevées : journalisation insuffisante, sauvegardes mal planifiées, dépendance à des technologies obsolètes, ou encore manque d'interopérabilité. Surtout, un constat récurrent est revenu : la sécurité n'est que rarement pensée dès la conception. La logique du « security by design » reste marginale, au profit d'un développement accéléré orienté résultat, notamment en méthode agile, où les mesures de sécurité sont souvent reléguées à la phase finale, voire absentes. Cette absence de sécurisation dès la genèse logicielle fragilise l'ensemble du dispositif, car un outil vulnérable à la base rend inefficace toute tentative de protection a posteriori du contenu archivé.

Aussi, nous sommes nous attardé à dégager des leviers d'amélioration.actuellement envisager sur le marché (blockchain, le wallet) afin d'analyser les avantages qu'offres ces derniers, mais aussi les éventuelles limites à leur implémentation dans le domaine des systèmes d'archivage numérique ; Et relever quelques recommandations visant non seulement à combler les lacunes observées, mais à poser les bases d'un système d'archivage électronique véritablement résilient, c'est-à-dire capable de résister, de s'adapter et d'évoluer dans un environnement mouvant.

Sur ce à la question de savoir si les SAE sont aujourd'hui suffisamment robustes, adaptatifs et sûrs pour répondre aux exigences contemporaines en matière de cybersécurité documentaire, nous ne pouvons répondre que de façon nuancée. En théorie, oui : les normes existent, les cadres sont définis, les bonnes pratiques sont connues. Mais dans la réalité, leur application est hétérogène. Certains éditeurs intègrent les exigences de sécurité dès les premières phases du développement, notamment dans les secteurs sensibles (juridique, défense, finance). D'autres, au contraire, peuvent livrer des produits fonctionnels mais fragiles, conçus dans une logique de performance minimale et de rentabilité, où les processus de cybersécurité sont bâclés ou ignorés.

Dans ce contexte, il serait inexact d'affirmer que les SAE sont aujourd'hui globalement robustes. Leur résilience dépend largement de la qualité de leur conception initiale, des pratiques de développement appliquées, et du niveau d'exigence des structures commanditaires. L'adaptabilité des SAE n'est pas impossible, mais elle suppose des investissements importants, parfois une refonte partielle, avec les risques que cela peut engendrer sur l'intégrité des données.

En définitive, tant que les bonnes pratiques de cybersécurité ne seront pas systématiquement intégrées dès la conception et tout au long du cycle de vie des systèmes, la robustesse des SAE restera relative. Il est donc impératif que les acteurs publics et privés exigent non seulement la conformité aux normes, mais aussi une véritable **cyber-hygiène de développement**. C'est à cette condition que les systèmes d'archivage électronique pourront évoluer en outils réellement protecteurs du patrimoine numérique, à la fois durables, adaptatifs et dignes de confiance.

Bibliographie

[1] PIAF – Portail International Archivistique Francophone, *Glossaire – Module 2*, [en ligne]. Disponible sur : https://www.piaf-archives.org/sites/default/files/bulk_media/glossairev3/co/Module_glossaire_2.html

[2] *Code du patrimoine*, articles L212-1 à L212-5, version consolidée 2024, Légifrance, [en ligne]. Disponible sur : https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006129161/

[3] *La mise en place d'un SAE*, dans *Archivage électronique : un nouveau domaine d'expertise au service de la gouvernance des systèmes d'information*, p. 15-19, [en ligne]. Disponible sur : https://123dok.net/article/mise-place-archivage-électronique-nouveau-domaine-expertise-service.yd7r5er1#google_vignette

[4] *Le SAE – Système d'Archivage Électronique*, [en ligne]. Disponible sur : https://www.archivage-numerique.fr/sae

[5] Office québécois de la langue française (OQLF), *Système d'information – Vocabulaire*, 1998, [en ligne]. Disponible sur : https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8358435/systeme-dinformation (consulté le 2 mai 2025).

[6] DESCHAMPS, Jules, *Comprendre la Norme Internationale pour l'Archivage Électronique*, 20 décembre 2024, [en ligne]. Disponible sur : https://www.transarchivistique.fr/comprendre-la-norme-internationale-pour-larchivage-electronique/#Le_modele_OAIS

[7] *Le coffre-fort numérique, une solution pérenne pour un archivage sécurisé de vos e-documents*, Silae, [en ligne]. Disponible sur : https://www.silae.fr/le-coffre-fort-numerique-une-solution-perenne-pour-un-archivage-securise/

[8] *Coffre-fort numérique : principe et fonctionnement*, Crédit Agricole, 31 mai 2024, [en ligne]. Disponible sur : https://www.credit-agricole.fr/particulier/conseils/magazine/tout-un-mag/pourquoi-utiliser-un-coffre-fort-numerique-pour-vos-documents-a-archiver.html

[9] SISAdemat, *La norme française NF Z42-020 sur le coffre-fort électronique*, 2023, [en ligne]. Disponible sur : https://www.sisademat.fr/normes/la-norme-francaise-nf-z42-020-sur-le-coffre-fort-electronique (consulté le 30 mai 2025).

[10] Parlement européen et Conseil de l'Union européenne, *Règlement (UE) 2024/1183 du 11 avril 2024*, [en ligne]. Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401183

[11] Fédération des Tiers de Confiance du Numérique (FNTC), *Comprendre le service qualifié d'archivage électronique*, mai 2025, [en ligne]. Disponible sur : https://fntc-numerique.com/wp-content/uploads/2025/04/Service-qualifie-darchivage-electronique.pdf

[12] CARON, Bertrand, *Formats de données pour la préservation à long terme : la politique de la BnF*, Bibliothèque Nationale de France, 2021. [Rapport technique]. Disponible sur : https://hal.archives-ouvertes.fr/hal-03374030v1

[13] SABOURIN, Jean-Luc, *Archiver l'information*, Université de la Rochelle, [en ligne]. Disponible sur : https://cours.unjf.fr/file.php/135/Cours/C2iD4-LutteCyberCrim/D4-4%20Sabourin/co/S03_G03.html

[14] *Les 5 grands principes de la sécurité informatique*, Le Bloc Note, 2023, [en ligne]. Disponible sur : https://www.leblocnote.fr/les_5_grands_principes_de_la_securite_informatique/ (consulté le 30 mai 2025).

[15] CNIL, *Règlement général sur la protection des données (RGPD) – Article 5 : Principes relatifs au traitement des données à caractère personnel*, [en ligne]. Disponible sur : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5

[16] Agence nationale de la sécurité des systèmes d'information (ANSSI), *Recommandations pour la protection des systèmes d'information essentiels*, [en ligne]. Disponible sur : https://cyber.gouv.fr/publications/recommandations-pour-la-protection-des-systemes-dinformation-essentiels

[17] GERARDIN, Claire, *La norme NF Z42-013 ou l'archivage électronique à valeur probatoire*, [en ligne]. Disponible sur : https://www.clairegerardin.com/wp-content/uploads/2016/05/eBook-Norme-NF-Z42-0131-1.pdf

[18] MEISSONNIER, Antoine, *Stockage des données électroniques, SAE et système d'information des archives*, 19 septembre 2014, [en ligne]. Disponible sur : https://siaf.hypotheses.org/279

[19] Agence nationale de la sécurité des systèmes d'information (ANSSI), *Guide pour l'élaboration d'une politique de sécurité des systèmes d'information*, [en ligne]. Disponible sur : https://cyber.gouv.fr/publications/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation

[20] ISO/IEC, *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*, 2013, [en ligne]. Disponible sur : https://cdn.standards.iteh.ai/samples/54534/986401bb9cb249deb71ce3bdd0c245d9/ISO-IEC-27001-2013.pdf

[21] SIBILLE-DE GRIMOUÄRD, C. ; NICHELE, B., « Le Standard d'échange de données pour l'archivage (SEDA), un outil structurant pour l'archivage », *La Gazette des archives*, n° 240, 2015-4, pp. 153-164, [en ligne]. Disponible sur : https://www.persee.fr/doc/gazar_0016-5522_2015_num_240_4_5291

[22] Direction de l'information légale et administrative (Premier ministre), *Obligations en matière de protection des données personnelles (RGPD)*, 26 avril 2024, [en ligne]. Disponible sur : https://entreprendre.service-public.fr/vosdroits/F24270

[23] *Le rôle essentiel d'un SAE face au RGPD*, Arkhineo, 12 février 2025, [en ligne]. Disponible sur : https://arkhineo.com/le-role-essentiel-dun-sae-face-au-rgpd/

[24] *Loi n° 2008-696 du 15 juillet 2008 relative aux archives*, Légifrance, [en ligne]. Disponible sur : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000019198529

[25] AFNOR Certification, *Certification ISO/IEC 27001 – Sécurité des systèmes d'information*, [en ligne]. Disponible sur : https://certification.afnor.org/numerique/certification-iso-27001

[26] *ISO/CEI 27001*, Wikipédia, [en ligne]. Disponible sur : https://fr.wikipedia.org/wiki/ISO/CEI_27001

[27] *Signature cryptographique : du numérique à l'électronique*, *La Lettre d'ADELI*, n°46, janvier 2002, [en ligne]. Disponible sur : https://espaces-numeriques.org/wp-content/uploads/2019/01/l46p23.pdf

[28] Sophos, *L'état des ransomwares 2024 : Résultats d'une étude indépendante et agnostique*, Livre blanc, avril 2024, [en ligne]. Disponible sur : https://www.campuscyber-na.fr/campus-api/uploads/sophos_state_of_ransomware_2024_wpfr_4995094a3f.pdf

[29] CrowdStrike, *Exemples de ransomwares : 16 attaques récentes de ransomwares*, [en ligne]. Disponible sur : https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-examples/

[30] Trend Micro, *15 exemples de ransomware : RansomHub*, [en ligne]. Disponible sur : https://www.trendmicro.com/fr_fr/what-is/ransomware/ransomware-examples.html

[31] ANSSI, *Ciblage et compromission d'entités françaises au moyen du mode opératoire d'attaque APT28 : Activités associées à APT28 depuis 2021*, CERT-FR, 29 avril 2025, version 1, 7 pages, [en ligne]. Disponible sur : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-006.pdf

[32] RIESS-MARCHIVE, Valéry, *Campagne MOVEit : SYNLab, Cegedim, Nuance, PwC… la litanie des victimes de Cl0p*, *Le MagIT*, 19 juin 2023, [en ligne]. Disponible sur : https://www.lemagit.fr/actualites/366542312/Campagne-MOVEit-SYNLab-Cegedim-Nuance-PwC-la-litanie-des-victimes-de-Cl0p (consulté le 12 mai 2025).

[33] *Un vol de données ébranle Fortinet, un géant de la cybersécurité*, 01net, [en ligne]. Disponible sur : https://www.01net.com/actualites/vol-donnees-ebranle-fortinet-geant-ybersecurite.html

[34] THIERRY, Gabriel, *Palmarès 2023 : le triste bilan du hack de MOVEit, le piratage le plus marquant de l'année*, *ZDNet*, 22 décembre 2023, [en ligne]. Disponible sur : https://www.zdnet.fr/actualites/palmares-2023-le-triste-bilan-du-hack-de-moveit-le-piratage-le-plus-marquant-de-l-annee-39963172.htm

[35] PAILLOT, Fabien, *Cyberattaque : l'agglomération Grand Cognac refuse de payer la rançon*, *Le Parisien*, 31 octobre 2019, [en ligne]. Disponible sur : https://www.leparisien.fr/societe/cyberattaque-l-agglomeration-grand-cognac-refuse-de-payer-la-rancon-31-10-2019-8183676.php

[36] BOHIC, Clément, *Ransomware : 3 infos sur l'attaque contre la Région Grand Est*, *Silicon.fr*, 24 février 2020, mis à jour le 2 avril 2025, [en ligne]. Disponible sur : https://www.silicon.fr/Thematique/cybersecurite-1371/Breves/ransomware-infos-attaque-region-grand-est-445177.htm

[37] *L'IA et le machine learning au service d'une cybersécurité préventive*, IT Pro Magazine, 3 juin 2025, [en ligne]. Disponible sur : https://www.itpro.fr/lia-et-le-machine-learning-au-service-dune-cybersecurite-preventive/

[38] CHEMINAT, Jacques, *Sur fond de cyberattaques, les plaintes à la Cnil repartent à la hausse*, *Le Monde Informatique*, 23 avril 2024, [en ligne]. Disponible sur : https://www.lemondeinformatique.fr/actualites/lire-sur-fond-de-cyberattaques-les-plaintes-a-la-cnil-repartent-a-la-hausse-93565.html

[39] *Redondance des données : guide pour améliorer la résilience de vos systèmes*, CastorDoc, 6 mars 2025, [en ligne]. Disponible sur : https://www.castordoc.com/data-strategy/redondance-des-donnees-guide-pour-ameliorer-la-resilience-de-vos-systemes

[40] Agence nationale de la sécurité des systèmes d'information (ANSSI), *Recommandations pour la protection des systèmes d'information essentiels*, 22 décembre 2020, mis à jour le 22 décembre 2020, [en ligne]. Disponible sur : https://cyber.gouv.fr/publications/recommandations-pour-la-protection-des-systemes-dinformation-essentiels

[41] ANSSI, *Anticiper et gérer une crise cyber*, publié le 20 juillet 2022, mis à jour le 29 février 2024, [en ligne]. Disponible sur : https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

[42] LAGAISSE, Kevin, *La blockchain, qu'est-ce que c'est ?*, 2025, [en ligne]. Disponible sur : https://kevin.lagaisse.fr/blockchain-quest-cest/

[43] *Qu'est-ce que la sécurité par conception (security by design)*, Unguess Newsroom, 13 octobre 2023, [en ligne]. Disponible sur : https://blog.unguess.io/fr/security-by-design

Bibliographie complémentaire

- ASSOCIATION DES ARCHIVISTES FRANÇAIS, *Abrégé d'archivistique : principes et pratiques du métier d'archiviste*, 4e éd., refondue et augmentée, Paris : Association des archivistes français, 2020, 348 p. ISBN 978-2-900175-09-5.

- MONTEL, Julien, *Étude et réalisation d'un prototype d'archivage électronique appliqué aux collectivités territoriales*, Mémoire d'ingénieur, CNAM Rennes, 2016, [en ligne]. Disponible sur : https://dumas.ccsd.cnrs.fr/dumas-01798631v1 (consulté le 30 mai 2025).

- MICAELLI, Éric, *Système d'archivage électronique (SAE)*, Archivistes-Experts, publié le 19 mars 2010, mis à jour le 10 mai 2012, [en ligne]. Disponible sur : https://www.archivistes-experts.fr (consulté le 2 mars 2025).

- Engen RDC, *Cahier des charges pour la mise en place d'un système de : Archivage, gestion électronique des documents, organisation & assainissement physiques des archives*, Réf. CDC/0523/ENGEN/RDC, validé par Mme Mamie Tima, Kinshasa, 2023, [en ligne]. Disponible sur : https://www.mediacongo.net/dpics/filesmanager/jobaof/2023/08-aout/02/engen_230807_01_01.pdf (consulté le 22 février 2025).

- BELIN, A. ; RIETSCH, J.-M., « Archivage électronique et analyse de risque : les nouveaux défis de l'archiviste », *Archives*, vol. 46, no 1, 2016, pp. 47–60, [en ligne]. Disponible sur : https://doi.org/10.7202/1035722ar.

- *Les systèmes d'archivage électronique ou SAE*, Quai des Entrepreneurs, [en ligne]. Disponible sur : https://www.quai-des-entrepreneurs.com/les-systemes-darchivage-electronique-ou-sae/

- [CONFÉRENCE 2013] *Archivage électronique des documents : le bon compromis*, [Vidéo en ligne]. Disponible sur : https://www.youtube.com/watch?v=IxAmkJEXJrI

- Archimag, *Confiance Numérique 2025 : De l'identité numérique à l'archivage électronique : Comment sécuriser votre écosystème numérique*, webinaire du jeudi 22 mai à 09h30, [en ligne]. Disponible sur : https://app.livestorm.co/serda-archimag/confiance-numerique-2025/live?s=09fd463e-0813-4025-a7b5-f817c7ed2f56#/chat

Table des matières

Remerciements 3
Introduction Générale 6
PARTIE I 8
Cadre théorique : entre archivage numérique et cybersécurité 8
Chapitre 1 - Fondements et normalisation des systèmes d'archivage électronique 10
1.1 Définition et finalités d'un Système d'Archivage Électronique (SAE) 10
1.2 SAE vs coffre-fort électronique : distinctions et complémentarités 12
1.3 Le rôle des prestataires de confiance et la notion de SAE qualifié 14
1.4 Typologie des objets numériques à archiver et des enjeux autours 16
1.5 Normes et référentiels essentiels 18
Chapitre 2 - La sécurité dans les systèmes d'information et les SAE 20
2.1 Les grands principes de la sécurité informatique : fondements de la résilience documentaire dans les SAE 20
Confidentialité 21
Intégrité 21
Disponibilité 21
Traçabilité 22
Authentification 22
2.2 Architecture sécurisée d'un SAE 23
2.3 Cas particuliers : signature électronique, horodatage, empreinte numérique 25
2.4 Réglementation et gouvernance de la sécurité 27
Chapitre 3 - Menaces émergentes et vulnérabilités des SAE 30
3.1 Cartographie des cybermenaces 31
L'hameçonnage (phishing) : vecteur d'usurpation et d'infiltration 32
Les APT (Advanced Persistent Threats) : attaques furtives et prolongées 32
Les failles logicielles : vulnérabilités systémiques 32
L'IA : à la fois menace et opportunité 33
3.2 Études de cas de cyberattaques récentes touchant des administrations 34
3.3 Vulnérabilités liées à l'obsolescence technologique et à la pérennité des formats... 36
3.4 L'intelligence artificielle : risque émergent ou levier défensif pour les SAE ?..... 37
PARTIE II 41
Analyse critique et perspectives : vers une cybersécurisation durable des SAE 41

Chapitre 4 - Évaluation des capacités actuelles de défense des SAE 43
4.1 Présentation de Congo Digital Service, filiale congolaise de l'entreprise Alessya Consulting 43
4.2 Analyse critique des dispositifs existants 45
4.3 Analyse des politiques de sauvegarde, de redondance et de récupération après sinistre 46
4.4 Problèmes d'interopérabilité et de continuité d'exploitation 48
4.5 Lacunes en matière d'agilité et d'adaptation face aux menaces dynamiques 50
Chapitre 5 - Innovations et solutions émergentes pour renforcer la cybersécurité des SAE ... 52
5.1 Blockchain et archivage à valeur probatoire 52
5.2 Wallets numériques : une piste prometteuse pour la gestion d'identité et le partage sécurisé dans les SAE 54
5.3 Intelligence artificielle et cybersécurité prédictive : un déséquilibre entre acteurs défensifs et pirates 56
5.4 Standards européens et certification de confiance : une excellence à étendre, mais à rééquilibrer 57
Chapitre 6 - Recommandations pour une stratégie de résilience des SAE 59
6.1 Intégration des principes de cybersécurité dès la conception du SAE 59
6.2 Renforcement des audits de sécurité et de la gestion des vulnérabilités 61
6.3 Sensibilisation, formation et culture de la sécurité pour les archivistes 62
6.4 Vers un modèle de gouvernance adaptative et collaborative 64
Conclusion générale 67
Bibliographie 69
Table des matières 74
ANNEXES (volume 2) 76

ANNEXES (volume 2)

Compte rendu d'entretien du 16 mai 2025

Sources : Informaticiens de Congo Digital Service

Participants :

- Renée Elodie HOUNTOHOTEGBE, étudiante en Master 1
- Stévie TATHY, DevOps
- Gespère BONAZEBI, développeur Fullstack

Durée : Environ 1h30
Mode : Visioconférence

Introduction

Dans le cadre de ce mémoire de recherche, un entretien exploratoire a été mené le 16 mai 2025 avec deux professionnels informatiques de Congo Digital Service (DevOps et Développeurs fullstack), Stévie TATHY et Gespère BONAZEBI, dans le but de recueillir des observations de terrain sur la sécurité des systèmes d'archivage électronique (SAE). Ces deux intervenants disposent d'une expérience directe dans la gestion, l'audit et le développement de solutions GED/SAE. L'échange, a permis d'aborder les forces, les vulnérabilités et les perspectives d'évolution des dispositifs de sécurité des SAE. L'entretien s'est déroulé sous forme semi-directive, en suivant les grandes thématiques du guide d'entretien, tout en laissant place à des développements libres et spontanés.

1. Dispositifs de sécurité en place

Interrogés sur les mesures de sécurité qu'ils avaient pu constater dans les SAE audités ou utilisés, les deux informaticiens ont évoqué en premier lieu le chiffrement des données et la journalisation des accès comme pratiques courantes. Selon Stévie TATHY, le chiffrement garantit que même un accès au serveur n'offre pas de visibilité sur les données. La journalisation, quant à elle, permet une traçabilité complète des actions : connexions, déconnexions, modifications.

Gespère BONAZEBI a ajouté que dans certaines solutions internes, comme celle développée chez CDS, une attention est aussi portée à la sécurisation du transit des données et à l'encapsulation des accès au serveur.

En revanche, ils ont pointé plusieurs limites : une authentification parfois trop basique, l'absence de journalisation des tentatives de connexion échouées, et surtout le manque d'évolution des logiciels (interface vieillissante, mises à jour rares ou uniquement esthétiques).

2. Sauvegarde, redondance et reprise après sinistre

Concernant les politiques de sauvegarde, les intervenants ont bien distingué la sauvegarde (copie régulière des données sur un support sécurisé) et la redondance (mise en miroir des données sur un second serveur prêt à prendre le relais).

Ils ont expliqué que les SAE devraient théoriquement s'appuyer sur un Plan de Continuité d'Activité (PCA), mais qu'en pratique, ces plans sont rarement testés. Les entreprises supposent souvent à tort qu'en cas de cyberattaque, la reprise sera fluide. Or, sans simulation préalable, la restauration des données peut s'avérer partielle ou défaillante.

3. Interopérabilité et évolutivité des SAE

Sur la question de l'interopérabilité, Gespère BONAZEBI a indiqué ne pas avoir rencontré de difficultés majeures, ayant principalement utilisé des solutions d'un même éditeur (ex. Maarch Courrier avec OnlyOffice). Cependant, Stévie TATHY a précisé que des limitations pouvaient apparaître lorsque des solutions extérieures devaient communiquer (ex : avec Active Directory).

Concernant l'évolutivité, tous deux s'accordent à dire que certaines solutions, notamment les SAE du marché, évoluent peu et n'intègrent que rarement les nouveaux standards de sécurité. En revanche, des outils développés en interne peuvent gagner en souplesse, car les équipes peuvent y intégrer des exigences spécifiques.

4. Capacité d'adaptation face aux menaces

Interrogés sur la capacité des SAE à faire face aux nouvelles cybermenaces, les deux participants ont insisté sur le retard de certaines solutions. Gespère BONAZEBI note que les

mises à jour ne renforcent pas toujours la sécurité : elles se concentrent parfois sur l'interface ou de nouvelles fonctionnalités, sans prise en compte des menaces récentes.

Les intervenants ont dénoncé une culture de la réaction : tant qu'aucun incident n'a lieu, les mises à jour de sécurité sont négligées. Ils appellent à intégrer la veille technologique comme une obligation continue, pour éviter que des failles connues soient exploitées.

Parmi les améliorations recommandées, ils citent :

- La double authentification (via application ou code temporaire) à l'image de Authentificator,
- L'alerte automatique en cas de comportement suspect (tentatives multiples de connexion),
- Le renforcement de la sécurité des formulaires pour éviter les injections de code.

5. Perspectives technologiques : wallets numériques et IA

À propos des wallets numériques, les deux experts ont évoqué un intérêt théorique : ils pourraient offrir un moyen sécurisé d'identifier un usager en lui demandant l'accès à son portefeuille d'identité. Ce système, encore peu répandu, soulève cependant des freins techniques et économiques.

Quant à l'intelligence artificielle, les participants reconnaissent son potentiel en cybersécurité prédictive, notamment pour détecter des comportements anormaux. Toutefois, ils soulignent que les SAE n'intègrent pas ce type d'outils et que les compétences en IA restent peu maîtrisées dans le monde de l'archivage.

6. Gouvernance, conception et culture de la sécurité

Sur la prise en compte de la cybersécurité dès la conception, les participants ont rappelé qu'en théorie, la sécurité doit être intégrée dès la phase de développement. En pratique, cela n'est pas systématique. Lorsque les mesures sont ajoutées après coup, cela alourdit le développement et fragilise l'ensemble.

Ils reconnaissent également l'absence de processus clair de gestion des vulnérabilités post-déploiement. En cas de faille, la réponse dépend souvent du bon vouloir ou de la réactivité de

l'équipe. Certains bugs ne sont pas anticipés car jamais reproduits lors des tests. Des utilisateurs malveillants peuvent ainsi injecter du code via des champs non sécurisés.

Enfin, sur la culture de la sécurité, ils jugent que les archivistes sont peu sensibilisés à ces enjeux. La formation initiale ne couvre pas ces aspects, et la collaboration avec les informaticiens est encore trop superficielle. Ils recommandent de renforcer les formations, y compris par des mises en situation simulées (phishing, alertes, fausses cyberattaques).

Conclusion de l'entretien

En guise de recommandation stratégique finale, Stévie TATHY a souligné la nécessité d'intégrer la sécurité dès la conception, de maintenir une veille technologique active et de respecter les normes en continu. Gespère BONAZEBI a insisté sur l'importance d'alerter en cas de comportement suspect, de renforcer la double authentification, et de tester régulièrement les dispositifs de sauvegarde.